RESULT LIST
2 results found in the Worldwide database for:
jp2000285024 (priority or application number or publication number)
(Results are sorted by date of upload in database)

1 **PRINTER, PRINTING SYSTEM, PRINTING METHOD, AND RECORDING MEDIUM WITH PRINTING PROGRAM RECORDED THEREIN**

Inventor: FUJII MASAHITO **Applicant:** MINOLTA CO LTD

EC: **IPC:** ***B41J21/00; G06F3/12; H04N1/387*** (+6)

Publication info: **JP2002086835** - 2002-03-26

2 **METHOD FOR ELECTRONICALLY STORING ORIGINAL GUARANTEE AND COMPUTER READABLE RECORDING MEDIUM RECORDING PROGRAM FOR EXECUTING THE METHOD BY COMPUTER**

Inventor: KANAI YOICHI; YANAIDA MASUYOSHI; (+2) **Applicant:** RICOH KK; NEW MEDIA DEV ASS

EC: **IPC:** ***G06F12/00; G06F12/14; G09C1/00*** (+9)

Publication info: **JP2000285024** - 2000-10-13

Data supplied from the ***esp@cenet*** database - Worldwide

METHOD FOR ELECTRONICALLY STORING ORIGINAL GUARANTEE AND COMPUTER READABLE RECORDING MEDIUM RECORDING PROGRAM FOR EXECUTING THE METHOD BY COMPUTER

Patent number: JP2000285024

Publication date: 2000-10-13

Inventor: KANAI YOICHI; YANAIDA MASUYOSHI; SUGAO KIYOSHI; TOZAKI HIDEKAZU

Applicant: RICOH KK; NEW MEDIA DEV ASS

Classification:

- international: ***G06F12/00; G06F12/14; G09C1/00; H04L9/32;*** **G06F12/00; G06F12/14; G09C1/00; H04L9/32;** (IPC1-7): G06F12/14; G06F12/00; G09C1/00; H04L9/32

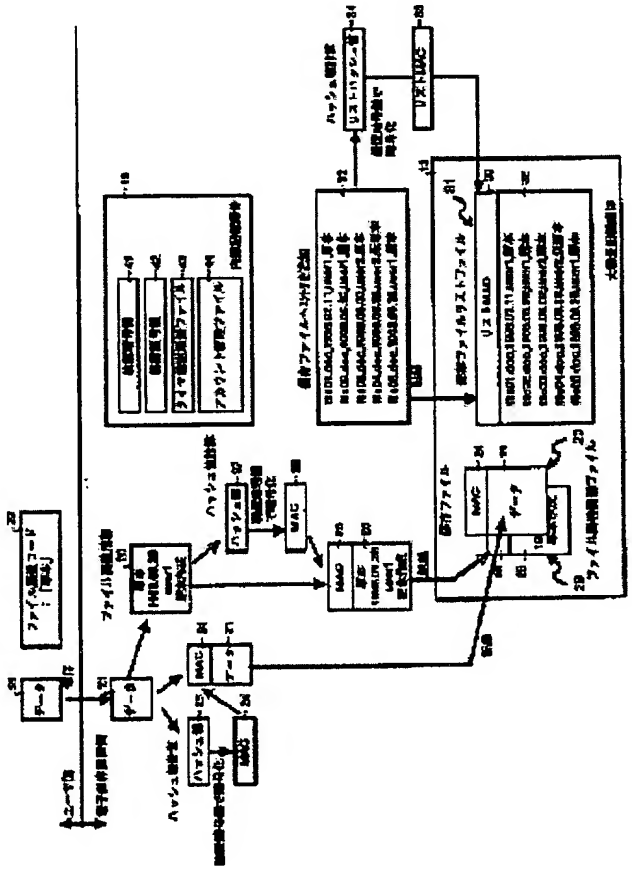
- european:

Application number: JP19990090212 19990330

Priority number(s): JP19990090212 19990330

Abstract of **JP2000285024**

PROBLEM TO BE SOLVED: To improve the certification ability of electronic information by providing the electronic information with properties included in a paper original. SOLUTION: In the case of storing electronic data 21, a file attribute code 22 indicating an original is added to the data 21 and the data 21 are stored in a state capable of discriminating it at least from other electronic data. The control level of an access to the original electronic data and the control level of an access to other electronic data can be respectively controlled.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－285024
（P2000－285024A）
(43)公開日　平成12年10月13日(2000.10.13)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
G06F	12/14	310	G06F	12/14	310K　5B017
	12/00	537		12/00	537A　5B082
G09C	1/00	640	G09C	1/00	640D　5J104
		660			660D　9A001
H04L	9/32		H04L	9/00	675A

審査請求　未請求　請求項の数10　ＯＬ　（全 26 頁）

(21)出願番号　特願平11－90212

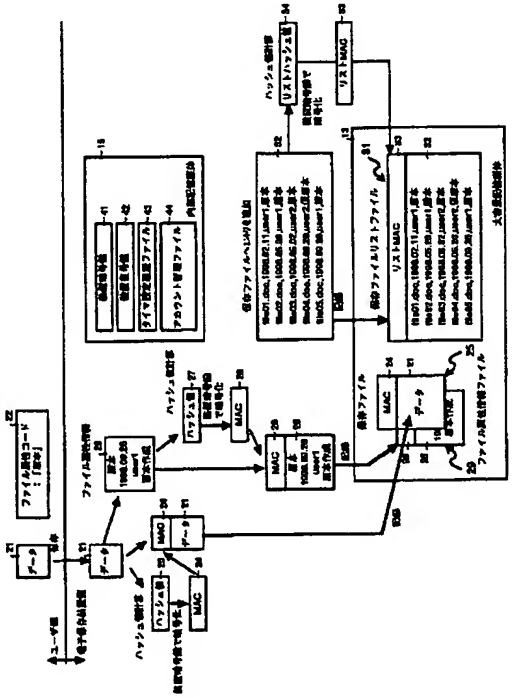
(22)出願日　平成11年３月30日(1999.3.30)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(71)出願人　596062738
財団法人ニューメディア開発協会
東京都港区三田１－４－28
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100089118
弁理士　酒井　宏明

最終頁に続く

(54)【発明の名称】　原本性保証電子保存方法およびその方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　紙の原本が有する性質を電子情報に持たせ、電子情報の証明力を高めること。
【解決手段】　電子データ２１を保存する際に、原本であることを示すファイル属性コード２２を付加し、少なくとも他の電子データとを識別可能な状態で保存するようにする。そして、原本の電子データに対するアクセス制御のレベルおよびその他の電子データに対するアクセス制御のレベルを制御可能にする。



【特許請求の範囲】
【請求項１】　電子データを保存する際に、少なくとも原本の電子データとその他の電子データとを識別可能な状態で保存し、前記原本の電子データに対するアクセス制御のレベルおよびその他の電子データに対するアクセス制御のレベルを制御することを特徴とする原本性保証電子保存方法。
【請求項２】　前記電子データは、対応する属性情報と共に保存され、
前記属性情報は、ユーザが編集入力を行えないように管理されており、
前記原本の電子データに対し、前記属性情報として原本であることを示す属性コードを付与することを特徴とする請求項１に記載の原本性保証電子保存方法。
【請求項３】　さらに、前記原本の電子データに対する修正履歴を記録することを特徴とする請求項１または２に記載の原本性保証電子保存方法。
【請求項４】　さらに、前記原本の電子データに対する削除処理の実行を禁止することを特徴とする請求項１または２に記載の原本性保証電子保存方法。
【請求項５】　さらに、前記原本の電子データの複製を生成し、生成した複製を前記原本に対する謄本として管理することを特徴とする請求項１または２に記載の原本性保証電子保存方法。
【請求項６】　さらに、前記原本の電子データの作成もしくは修正した順番または時刻に関する情報を、外部から変更できないようにするか、または変更されても変更された事実を検出可能な状態で、前記原本の電子データと共に保存することを特徴とする請求項１または２に記載の原本性保証電子保存方法。
【請求項７】　さらに、前記電子データの移動が要求された場合に、前記電子データを対応する属性情報と共に移動させることを特徴とする請求項２に記載の原本性保証電子保存方法。
【請求項８】　さらに、前記原本または謄本の電子データおよび対応する属性情報にメッセージ認証子を付与して保存し、前記電子データがアクセスされた場合に、前記メッセージ認証子を用いて前記電子データに対する改ざんを検出することを特徴とする請求項２に記載の原本性保証電子保存方法。
【請求項９】　さらに、第１の保存装置に存在する前記電子データの複製を第２の保存装置に生成するための要求または前記第１の保存装置に存在する前記電子データを前記第２の保存装置に移動させるための要求があった場合に、第１の保存装置は、前記電子データおよび対応する属性情報のそれぞれに付与された前記メッセージ認証子を検証した後、前記メッセージ認証子を除いた電子データおよび対応する属性情報を前記第２の保存装置に転送し、前記第２の保存装置は、前記電子データおよび対応する属性情報を受け取り、処理内容に応じて前記属性情報を変更し、前記電子データおよび対応する属性情報に対してメッセージ認証子を付与して保存することを特徴とする請求項２に記載の原本性保証電子保存方法。
【請求項１０】　前記請求項１～９のいずれか一つに記載の原本性保証電子保存方法をコンピュータに実行させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、原本性保証電子保存方法に関し、より詳細には、紙の原本が有する性質を電子情報に持たせ、電子情報の証明力を高めることが可能な原本性保証電子保存方法およびその方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。
【０００２】
【従来の技術】情報の電子化の時代における情報管理の考え方として、セキュリティ（Security）とトラスティ（Trusty）というものがある。セキュリティとは、外部からのアタックにより電子情報が破壊されたり、盗まれてしまうことから防衛することである。一方、トラスティとは、電子情報が紙情報に比べて簡単に改ざんすることが可能である点に鑑み、電子情報の改ざんを防止することによって電子情報の証拠能力を確保することである。
【０００３】上記トラスティには、第１の目的として、企業等の組織活動または個人活動が他より早く行われていたことを証明するという目的がある（優先権の主張）。ここで、第１の目的を達成するには、電子情報とその付随情報（作成時期等）が改ざん不可能となっているか、または改ざんされても改ざんの事実を確実に検知できるようになっていることが必要である。現在、この目的に対する実用的な解としては、ＴＴＰ（Trusted Third Party；第三者認証機関）があり、その代表的なものとしては、米国のＳｕｒｅｔｙ者が提供している認証サービスがある。
【０００４】また、トラスティには、第２の目的として、企業等の組織活動または個人活動として不正が行われていないことを証明するという目的がある。ここで、第２の目的を達成するには、電子情報とその付随情報（作成時期等）が改ざん不可能となっているか、または改ざんされても改ざんの事実を確実に検知できるようになっていることに加えて、電子情報ファイルが削除不可能または削除されたことが検知可能であることが必要である。この第２の目的は、環境や製造物責任等に対する企業の経営情報管理，官公庁等の情報公開等により今後ますます高くなってくると考えられている。この第２の目的を実現するためには、追記，修正等のバージョンアップや不正なファイル削除を防止するための機能が必要で、例えばローカルネットワークにおいて、ファイル管

理システムと一体化または連携した認証機能を有するシステムを用意することが好ましい。

【0005】

【発明が解決しようとする課題】ところで、現在は紙文書として保存することが法律で義務付けられている情報が多々存在しており、これが情報の電子化を阻害する要因となっているが、情報に原本性保証機能（真性性，保存性，見読性，原本の唯一性）を付与することにより、電子化が認められることになった（参照：総務庁通達等）。したがって、電子情報においても、紙ベースで構築されてきた法律体系に応じて原本と謄本とを区別できるようにすると共に、改ざんを容易に行えないようにし、電子情報の証明力を高めることが可能な技術の開発が望まれている。

【0006】また、原本性保証の対象となる情報は、前述した第2の目的に属する情報が大半であることから、ファイル管理システムと同じローカルエリアネットワーク上に存在する原本性保証サーバ、即ち、ユーザサイトに設置することが可能な原本性保証機能を有する認証サーバの実現が望まれている。これにより、例えば諸官庁の情報を扱うのに十分なトラスティとセキュリティを有した原本性保証サーバの実現が可能となる。

【0007】本発明は上記に鑑みてなされたものであって、紙の原本が有する性質を電子情報に持たせ、電子情報の証明力を高めることを可能にすることを目的とする。

【0008】また、本発明は上記に鑑みてなされたものであって、ユーザサイトに設置可能な原本性保証機能を有する認証サーバを実現可能にすることを目的とする。

【0009】

【課題を解決するための手段】上記目的を達成するため、請求項1の原本性保証電子保存方法は、電子データを保存する際に、少なくとも原本の電子データとその他の電子データとを識別可能な状態で保存し、前記原本の電子データに対するアクセス制御のレベルおよびその他の電子データに対するアクセス制御のレベルを制御するものである。

【0010】また、請求項2の原本性保証電子保存方法は、請求項1に記載の原本性保証電子保存方法において、前記電子データが、対応する属性情報と共に保存され、前記属性情報が、ユーザが編集入力を行えないように管理されており、前記原本の電子データに対し、前記属性情報として原本であることを示す属性コードを付与するものである。

【0011】また、請求項3の原本性保証電子保存方法は、請求項1または2に記載の原本性保証電子保存方法において、さらに、前記原本の電子データに対する修正履歴を記録するものである。

【0012】また、請求項4の原本性保証電子保存方法は、請求項1または2に記載の原本性保証電子保存方法において、さらに、前記原本の電子データに対する削除処理の実行を禁止するものである。

【0013】また、請求項5の原本性保証電子保存方法は、請求項1または2に記載の原本性保証電子保存方法において、さらに、前記原本の電子データの複製を生成し、生成した複製を前記原本に対する謄本として管理するものである。

【0014】また、請求項6の原本性保証電子保存方法は、請求項1または2に記載の原本性保証電子保存方法において、さらに、前記原本の電子データの作成もしくは修正した順番または時刻に関する情報を、外部から変更できないようにするか、または変更されても変更された事実を検出可能な状態で、前記原本の電子データと共に保存するものである。

【0015】また、請求項7の原本性保証電子保存方法は、請求項2に記載の原本性保証電子保存方法において、さらに、前記電子データの移動が要求された場合に、前記電子データを対応する属性情報と共に移動させるものである。

【0016】また、請求項8の原本性保証電子保存方法は、請求項2に記載の原本性保証電子保存方法において、さらに、前記原本または謄本の電子データおよび対応する属性情報にメッセージ認証子を付与して保存し、前記電子データがアクセスされた場合に、前記メッセージ認証子を用いて前記電子データに対する改ざんを検出するものである。

【0017】また、請求項9の原本性保証電子保存方法は、請求項2に記載の原本性保証電子保存方法において、さらに、第1の保存装置に存在する前記電子データの複製を第2の保存装置に生成するための要求または前記第1の保存装置に存在する前記電子データを前記第2の保存装置に移動させるための要求があった場合に、第1の保存装置が、前記電子データおよび対応する属性情報のそれぞれに付与された前記メッセージ認証子を検証した後、前記メッセージ認証子を除いた電子データおよび対応する属性情報を前記第2の保存装置に転送し、前記第2の保存装置が、前記電子データおよび対応する属性情報を受け取り、処理内容に応じて前記属性情報を変更し、前記電子データおよび対応する属性情報に対してメッセージ認証子を付与して保存するものである。

【0018】さらに、請求項10のコンピュータ読み取り可能な記録媒体は、前記請求項1～9のいずれか一つに記載の原本性保証電子保存方法をコンピュータに実行させるためのプログラムを記録したものである。

【0019】

【発明の実施の形態】以下、本発明に係る原本性保証電子保存方法およびその方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体の一実施の形態について、添付の図面を参照しつつ詳細に説明する。

【００２０】図１は、本実施の形態に係る原本性保証電子保存方法を実行する電子保存装置のブロック構成図である。ユーザは、ホスト計算機２側からネットワーク（単なる通信路で良い）を介して電子保存装置１に対して電子データの保存処理や読み出し処理を実行することができる。

【００２１】図１に示す電子保存装置１において、１１はプロセッサを、１２はネットワークを介して計算機２と通信を行うための通信ポートを、１３は電子データを保存するハードディスクやＣＤ－Ｒ等の大容量記憶媒体を、１４は主制御プログラム，ハッシュプログラム，鍵生成プログラム，暗号化プログラム，復号プログラム等の原本性保証電子保存方法を実現するためのプログラムが格納されたＥＥＰＲＯＭ，ＲＯＭ等で構成されたプログラム格納媒体を、１５は装置暗号鍵，装置復号鍵，タイマ設定履歴ファイル，アカウント管理ファイル等が記憶されるＥＥＰＲＯＭ等で構成された内部記憶媒体を、１６はアカウント名，ユーザ側内部認証鍵，ユーザ側外部認証鍵等が記憶されたＩＣカード３が挿入されるＩＣカードリーダ／ライタを、１７はタイマをそれぞれ示している。

【００２２】図１に示す大容量記憶媒体１３としては、光磁気ディスクやＣＤ－Ｒのように電子保存装置１から取り外し可能なものであっても良いが、その他のブロックは電子保存装置１として物理的に一体化されており、通信ポート１２を介する以外に外部からアクセスできないように構成されている。すなわち、図１に示す電子保存装置１は、各ブロックに対して直接アクセスする方法のない耐タンパー性を持った装置である。

【００２３】耐タンパー性を確保するレベルとしては、電子保存装置１の筐体を開けることができないようにシールを貼る程度のものから、筐体を開けられてしまった場合には装置が動作しなくなるようなものまで考えられるが、耐タンパー性を持たせることが可能であればどのようなものであっても良い。

【００２４】図１に示す電子保存装置１は、ユーザから保存要求のあったデータを大容量記憶媒体１３に記録するものである。その際、後にデータの改ざんを検出できるようにするため、保存するデータに対して電子保存装置１自身の暗号鍵によりメッセージ認証子を付加する。また、電子保存装置１は、大容量記憶媒体１３に記録されているファイルのリストを作成し、それを大容量記憶媒体１３に記録する処理を行う。このリストに対しても、同様にメッセージ認証子を付加する。

【００２５】また、大容量記録媒体１３の不正なすり替えを検出するために、大容量記憶媒体１３に記録されている保存ファイルリストと、それに付加されたメッセージ認証子を検出することで媒体の認証を行う。また、ファイルの作成日などに不正ができないよう、電子保存装置１に内蔵されているタイマ１７から現在時刻を取得し、ファイルの属性情報として管理する。

【００２６】さらに、電子保存装置１内部で、オリジナルとコピーとを区別することができるように、各ファイルには「仮原本」，「原本」，「謄本」といった属性を付与して管理する。属性の付与されていないファイルは「一般」ファイルと呼ぶことにする。「原本」の属性が付与されて管理されているファイルに対し、外部から複製の作成を要求すると、複製されたファイルには「謄本」という属性が付与される。この属性コードは、他のファイル属性情報と共に、データファイルと関連付けられたファイル属性情報ファイルとして大容量記憶媒体１３に記録され、データファイルと同様、メッセージ認証子を付加して外部から変更することができないように管理される。大容量記憶媒体１３を取り外して外部でその属性が改ざんされたような場合には、そのファイル属性情報ファイルに付与したメッセージ認証子を検証した際にその改ざんを検出することができる。

【００２７】つぎに、前述した構成を有する電子保存装置１を用いて実行される原本性保証電子保存方法について、

（１）ユーザ登録処理
（２）保存装置へのログイン処理
（３）電子データ保存処理
（４）大容量記憶媒体マウント処理
（５）ファイル読み出し処理
（６）謄本作成処理
（７）バックアップ作成処理
（８）ファイル移動処理
（９）ファイル削除処理
（１０）ファイル属性コード変更処理
（１１）ファイル追記処理
（１２）ファイル編集処理

の順で具体的に説明する。

【００２８】（１）ユーザ登録処理

ここでは、ユーザが電子保存装置１を利用する際に、電子保存装置１とユーザとの間で相互認証を行う必要があるものとする。そのため、電子保存装置１に対して予めユーザ登録を行っておく必要がある。ここで、電子保存装置１には、予めシステム管理者用のＩＣカードが付属しているものとする。クライアント（計算機２）に接続されたＩＣカードリーダにシステム管理者用のＩＣカードを挿入してアカウント登録用のプログラムを起動し、ユーザ登録を行う。

【００２９】図２は、ユーザ登録処理を示すフローチャートであり、図２（ａ）はクライアント側で実行されるユーザ登録処理を、図２（ｂ）は電子保存装置１側で実行されるユーザ登録処理をそれぞれ示している。以下では、図２（ａ）および図２（ｂ）の両方を用いてユーザ登録処理を説明する。

【００３０】まず、図２（ａ）に示すように、システム

管理者用ＩＣカードをクライアントのカードリーダに挿入し（Ｓ１１）、パスワードを入力する（Ｓ１２）。そして、ＩＣカードでパスワード照合が行われ（Ｓ１３）、正しいパスワードでない、即ち不正なパスワードの場合（Ｓ１４；Ｎｏ）、エラーとしてユーザ登録処理が終了となる。

【００３１】一方、正しいパスワードの場合（Ｓ１４；Ｙｅｓ）、図２（ａ）および図２（ｂ）に示すように、電子保存装置１およびＩＣカードとの間で相互認証処理が実行される（Ｓ１５，Ｓ２１）。そして、電子保存装置１およびＩＣカードとの間で実行された相互認証処理が成功しなかった場合（Ｓ１６，Ｓ２２；Ｎｏ）、エラーとしてユーザ登録処理が終了となる。

【００３２】また、電子保存装置１およびＩＣカードとの間で実行された相互認証処理が成功した場合（Ｓ１６，Ｓ２２；Ｙｅｓ）、クライアントから電子保存装置１に対してユーザ登録が要求される（Ｓ１７）。電子保存装置１は、クライアントからのユーザ登録の要求がシステム管理者からの要求か否かを判定し（Ｓ２３）、システム管理者からの要求ではないと判定した場合（Ｓ２３；Ｎｏ）、エラーとしてユーザ登録処理が終了となる。一方、システム管理者からの要求であると判定した場合（Ｓ２３；Ｙｅｓ）、電子保存装置１は、ユーザ登録要求からアカウント名を取得する（Ｓ２４）。ここで、新しいＩＣカードを電子保存装置１のＩＣカードリーダ／ライタ１６に挿入する（Ｓ２５）。

【００３３】電子保存装置１は、続いて、保存装置側外部認証鍵，ユーザ側内部認証鍵を生成すると共に（Ｓ２６）、ユーザ側外部認証鍵，保存装置側内部認証鍵を生成する（Ｓ２７）。つぎに、電子保存装置１は、四つの認証鍵，アカウント名等をまとめてユーザ情報とし、ユーザ情報をアカウント管理ファイルに登録する（Ｓ２８）。なお、アカウント管理ファイルは、図１に示した内部記憶媒体１５に記録されるものであって、例えば図３に示すような内容のものである。また、図３中に示す認証鍵情報および日時情報の内容がそれぞれ図４および図５に示されている。なお、図５に示す日時情報は、アカウント管理ファイルだけでなく、後述する各種ファイルにも含まれるものである。

【００３４】ここで、認証に使用される暗号アルゴリズムが秘密鍵暗号方式の場合には、保存装置側外部認証鍵とユーザ側内部認証鍵が同じ鍵となり、ユーザ側外部認証鍵と保存装置側内部認証鍵が同じ鍵となる。その一方、暗号アルゴリズムに公開鍵暗号方式を利用する場合には、保存装置側外部認証鍵とユーザ側内部認証鍵が対応するパブリックキーとプライベートキーとになり、ユーザ側外部認証鍵と保存装置側内部認証鍵が対応するパブリックキーとプライベートキーとになる。すなわち、外部認証鍵はパブリックキーに、内部認証鍵はプライベートキーになる。

【００３５】図２のフローチャートの説明に戻り、電子保存装置１は、ユーザ側内部認証鍵，ユーザ側外部認証鍵およびアカウント名をＩＣカードに設定し（Ｓ２９）、その後、ＩＣカードをＩＣカードリーダ／ライタ１６から排出し（Ｓ３０）、ユーザ登録処理を終了する。一方、図２（ａ）に示すように、クライアント側においては、ステップＳ１７で要求したユーザ登録要求が成功したか否かを判定し（Ｓ１８）、要求が成功しなかった場合（Ｓ１８；Ｎｏ）にはエラーとしてユーザ登録処理を終了し、要求が成功した場合（Ｓ１８；Ｙｅｓ）には正常にユーザ登録処理を終了する。

【００３６】なお、新しいＩＣカードには予めユーザパスワードが初期値として設定されている。初期値のパスワードを照合すると任意のパスワードに変更することが可能である。パスワード変更は、電子保存装置１とは関係なく、クライアント側で行うことができる。

【００３７】（２）電子保存装置へのログイン処理

電子保存装置１にファイルを保存したり、電子保存装置１からファイルを読み出す前に、ユーザは電子保存装置１にログインしなければならない。ログイン処理においては、ユーザ登録の際に発行されたＩＣカードを利用し、電子保存装置１との間で相互認証が行われる。ここでは、相互認証の方法として、公知の技術を採用することにする。

【００３８】図６は、電子保存装置１へのログイン処理を示すフローチャートであり、図６（ａ）はクライアント側で実行されるログイン処理であり、図６（ｂ）は電子保存装置１側で実行されるログイン処理である。図６（ａ）において、ログインユーザ用ＩＣカードをクライアントのカードリーダに挿入し（Ｓ３１）、パスワードを入力する（Ｓ３２）。

【００３９】ＩＣカードでパスワード照合が行われ（Ｓ３３）、正しいパスワードであるか否か、換言すれば、パスワードが不正でないか否かが判定される（Ｓ３４）。パスワードが不正であると判定された場合（Ｓ３４；Ｎｏ）、ログイン処理がエラーにより終了する。一方、パスワードは不正ではないと判定された場合（Ｓ３４；Ｙｅｓ）、図６（ａ）および図６（ｂ）にそれぞれ示すように、電子保存装置１およびＩＣカードとの間で相互認証処理が実行される（Ｓ３５，Ｓ４１）。なお、相互認証処理については後にフローチャートを用いて説明する。

【００４０】そして、相互認証処理に失敗した場合（Ｓ３６，Ｓ４２；Ｎｏ）、ログイン処理がエラーにより終了する。一方、相互認証処理に成功した場合（Ｓ３６，Ｓ４２；Ｙｅｓ）、電子保存装置１は乱数を生成し、生成した乱数をクライアントに送信し（Ｓ４３）、クライアントは電子保存装置１から送信された乱数を受信する（Ｓ３７）。

【００４１】クライアントは、受信した乱数をＩＣカー

ドに渡し、ユーザ側内部認証鍵で暗号化し（Ｓ３８）、暗号化乱数を電子保存装置１とのセッション鍵とする（Ｓ３９）。一方、電子保存装置１は、乱数をユーザ側内部認証鍵で暗号化し（Ｓ４４）、暗号化乱数をクライアントとのセッション鍵とする（Ｓ４５）。

【００４２】その後、クライアントは、暗号処理、メッセージ認証処理モードを送信し（Ｓ４０）、電子保存装置１は、暗号処理、メッセージ認証処理モードを受信し（Ｓ４６）、ログイン処理を正常に終了する。

【００４３】なお、クライアント側および電子保存装置１側のいずれとも、送信するデータにはセッション鍵を用いて生成したメッセージ認証子を付加し、また、受信したデータは同じくセッション鍵を用いてメッセージ認証子の検証処理を行う。また、クライアントから暗号処理モードを設定することが可能であり、暗号処理を行うように指定した場合には、クライアント側，電子保存装置１側とも、送信するデータをセッション鍵で暗号化し、また、受信したデータは同じくセッション鍵で復号する。

【００４４】図7は、図６（ａ）のステップＳ３５および図６（ｂ）のステップＳ４１において実行される相互認証処理のフローチャートであり、図７（ａ）はクライアント側で実行される相互認証処理を、図７（ｂ）は電子保存装置１側で実行される相互認証処理をそれぞれ示している。

【００４５】クライアントは、ＩＣカードからアカウント名を読み出し（Ｓ５１）、読み出したアカウント名を電子保存装置１に送信する（Ｓ５２）。電子保存装置１は、アカウント名を受信し（Ｓ６１）、アカウント管理ファイルを読み出す（Ｓ６２）。そして、電子保存装置１は、読み出したアカウント管理ファイルのアカウント管理データから該当するアカウント情報を取得する処理を行う（Ｓ６３）。ここで、該当するアカウント情報がアカウント管理データ中に存在しない場合（Ｓ６４；Ｎｏ）、相互認証処理はエラーにより終了する。

【００４６】一方、該当するアカウント情報がアカウント管理データ中に存在する場合（Ｓ６４；Ｙｅｓ）、電子保存装置１は乱数１を生成し（Ｓ６５）、生成した乱数１をクライアントに送信する（Ｓ６６）。

【００４７】クライアントは、乱数１を受信し（Ｓ５３）、受信した乱数１をＩＣカードに渡し、ユーザ側内部認証鍵で暗号化した認証コード１を取得する（Ｓ５４）。続いて、クライアントは、ＩＣカードで乱数２を生成し（Ｓ５５）、認証コード１と乱数２とを電子保存装置１に送信する（Ｓ５６）。

【００４８】電子保存装置１は、認証コード１と乱数２とを受信し（Ｓ６７）、保存装置側外部認証鍵で認証コード１を復号する（Ｓ６８）。そして、電子保存装置１は、復号した認証コードと乱数１とが一致するか否かを判定する（Ｓ６９）、ステップＳ６９において、一致しないと判定された場合（Ｓ６９；Ｎｏ）、相互認証処理がエラーにより終了する。一方、一致すると判定された場合（Ｓ６９；Ｙｅｓ）、ステップＳ７０において、電子保存装置１が乱数２を保存装置側内部認証鍵で暗号化して認証コード２を生成し（Ｓ７０）、認証コード２をクライアントに送信する（Ｓ７１）。

【００４９】クライアントは、認証コード２を受信し（Ｓ５７）、認証コード２をＩＣカードに渡し、ユーザ側外部認証鍵により外部認証を行う（Ｓ５８）。そして、外部認証が成功しなかった場合（Ｓ５９；Ｎｏ）、相互認証処理がエラーで終了し、外部認証が成功した場合（Ｓ５９；Ｙｅｓ）、相互認証処理が正常に終了し、図６のフローチャートの処理に戻ることになる。

【００５０】（３）電子データ保存処理

つぎに、電子データを電子保存装置１に保存する際の処理手順について説明する。図8は、電子データを電子保存装置１に保存する処理を示すフローチャートであり、図９は、原本データの保存処理の説明図である。以下では、図8のフローチャートに示す電子データ保存処理について、図９を参照しつつ具体的に説明する。

【００５１】電子保存装置１のプロセッサ１１は、通信ポート１２を介して計算機２から電子データの保存要求を受けた場合、大容量記憶媒体１３がマウントされているか否かを判定する（Ｓ８１）。ここで、大容量記憶媒体１３がマウントされていないと判定した場合（Ｓ８１；Ｎｏ）、プロセッサ１１は、エラーにより電子データ保存処理を終了する。

【００５２】一方、大容量記憶媒体１３がマウントされていると判定した場合（Ｓ８１；Ｙｅｓ）、通信ポート１２を介してユーザ側（計算機２）から、図９に示すデータ２１およびファイル属性コード２２を受け取る（Ｓ８２）。

【００５３】そして、プロセッサ１１は、受け取ったファイル属性コード２２が「原本」，「仮原本」または「一般」であるか否かを判定する（Ｓ８３）。ここで、ファイル属性コード２２が「原本」，「仮原本」または「一般」でないと判定した場合（Ｓ８３；Ｎｏ）、プロセッサ１１は、エラーにより電子データ保存処理を終了する。

【００５４】一方、ファイル属性コード２２が「原本」，「仮原本」または「一般」であると判定した場合（Ｓ８３；Ｙｅｓ）、プロセッサ１１は、ファイル属性コードが「一般」か否かを判定する（Ｓ８４）。ファイル属性コードが「一般」であると判定した場合（Ｓ８４；Ｙｅｓ）、プロセッサ１１は、受け取ったデータ２１を大容量記憶媒体１３にファイルとして保存し（Ｓ９２）、電子データ保存処理を正常に終了する。

【００５５】また、ファイル属性コードが「一般」ではないと判定した場合（Ｓ８４；Ｎｏ）、プロセッサ１１は、タイマ１７から現在時刻を取得すると共に、内部記

憶媒体１５から装置暗号鍵４１，装置復号鍵４２，最新タイマＩＤを取得し（Ｓ８５）、改ざん検知保存処理を実行してデータを大容量記憶媒体１３に保存する（Ｓ８６）。

【００５６】図１０は、ステップＳ８６の改ざん検知保存処理を示すフローチャートである。プロセッサ１１は、保存するデータ２１に対してハッシュ値を計算してハッシュ値２３を求め（Ｓ１０１）、ハッシュ値２３を装置暗号鍵４１で暗号化してメッセージ認証子（ＭＡＣ）２４を生成する（Ｓ１０２）。その後、メッセージ認証子２４と共にデータ２１を保存ファイル２５として大容量記憶媒体１３に保存する（Ｓ１０３）。

【００５７】図８のフローチャートに戻り、プロセッサ１１は、ファイル属性コード２２に対して現在時刻，ユーザアカウント名，ファイルアクセス履歴等を加えたファイル属性情報２６を生成し（Ｓ８７）、図１０に示したような改ざん検知保存処理を実行して、ファイル属性情報２６を大容量記憶媒体１３に保存する（Ｓ８８）。

【００５８】このステップＳ８８において実行される改ざん検知保存処理を図９および図１０を参照して説明する。プロセッサ１１は、図８のステップＳ８７で生成したファイル属性情報２６に対してハッシュ値を計算してハッシュ値２７を求め（Ｓ１０１）、ハッシュ値２７を装置暗号鍵４１で暗号化してメッセージ認証子（ＭＡＣ）２８を生成する（Ｓ１０２）。その後、メッセージ認証子２８と共にファイル属性情報２６をファイル属性情報ファイル２９として大容量記憶媒体１３に保存する（Ｓ１０３）。

【００５９】再び図８のフローチャートの説明に戻り、プロセッサ１１は、改ざん検知読み出し処理を実行して、大容量記憶媒体１３から保存ファイルリストファイル３１を読み出す（Ｓ８９）。

【００６０】図１１は、図８のステップＳ８９において実行される改ざん検知読み出し処理を示すフローチャートである。プロセッサ１１は、大容量記憶媒体１３に記録されている保存ファイルリストファイル３１（対象ファイル）を読み出し（Ｓ１１１）、保存ファイルリストファイル３１に記録されている保存ファイルリスト３２（データ）とメッセージ認証子（リストＭＡＣ）３１とを分離する（Ｓ１１２）。プロセッサ１１は、ステップＳ１１２で分離した保存ファイルリスト３２に対してハッシュ値を計算する（Ｓ１１３）。

【００６１】続いて、プロセッサ１１は、内部記憶媒体１５から装置復号鍵４２を取得し（Ｓ１１４）、取得した装置復号鍵４２でメッセージ認証子３３を復号して検証用ハッシュ値を求める（Ｓ１１５）。プロセッサ１１は、その後、ステップＳ１１３で求めたハッシュ値とステップＳ１１５で求めた検証用ハッシュ値とが一致するか否かを判定する（Ｓ１１６）。

【００６２】ステップＳ１１６において、二つのハッシュ値が一致しないと判定した場合（Ｓ１１６；Ｎｏ）、図８には詳細に示されていないが、プロセッサ１１はエラーとして改ざん検知読み出し処理および電子データ保存処理を終了する。一方、二つのハッシュ値が一致すると判定した場合（Ｓ１１６；Ｙｅｓ）、プロセッサ１１は、保存ファイルリスト３２を読み出しデータとし（Ｓ１１７）、図８のステップＳ９０に進む。

【００６３】再び図８のフローチャートの説明に戻り、プロセッサ１１は、読み出した保存ファイルリスト３２に保存ファイル２５のエントリを追加する（Ｓ９０）。そして、プロセッサ１１は、改ざん検知保存処理を実行して、保存ファイルリスト３２を大容量記憶媒体１３に記録し（Ｓ９１）、電子データ保存処理を終了する。

【００６４】なお、ステップＳ９１において実行される改ざん検知保存処理を図９および図１０を参照して説明する。プロセッサ１１は、Ｓ９０で保存ファイル２５のエントリが追加された保存ファイルリスト３２に対してハッシュ値を計算してリストハッシュ値３４を求め（Ｓ１０１）、リストハッシュ値３４を装置暗号鍵４１で暗号化してメッセージ認証子（リストＭＡＣ）３３を生成する（Ｓ１０２）。その後、メッセージ認証子３３と共に保存ファイルリスト３２を保存ファイルリストファイル３１として大容量記憶媒体１３に保存する（Ｓ１０３）。

【００６５】なお、図９に示した各種情報の内容について簡単に示すことにする。図１２は保存ファイル２５の内容を示す説明図であり、図１３はファイル属性情報ファイル２９の内容を示す説明図であり、図１４は保存ファイルリストファイル３１の内容を示す説明図であり、図１５はタイマ設定履歴ファイル４３の内容を示す説明図である。また、図９の内部記憶媒体１５に示すアカウント管理ファイル４４は図３に示したものに該当する。

【００６６】また、ここで、電子保存装置１における日時の管理について説明する。図１３に示したファイル属性情報ファイル２９中のファイルアクセス履歴等に記録する日時は、電子保存装置１内部のタイマ１７から取得するものであるが、ここではタイマ１７の設定を変更することができるようになっているものとする。そのため、タイマ１７を不正に変更することによりファイルアクセス日時を偽ることを防止するため、タイマ１７の設定を変更した履歴を記録するようにしている。タイマ１７の設定を変更すると、概念的には図１６に示すような履歴が内部記憶媒体１５のタイマ設定履歴ファイル４３に記録される。

【００６７】タイマＩＤは、電子保存装置１内部で自動的に振られるシーケンシャルな番号であり、タイマ１７の設定を変更するたびに番号が増えていく。なお、ファイルアクセス履歴に含まれる日時情報には図５に示したようにタイマＩＤが含まれている。

【００６８】図１６に示すようなタイマ設定履歴によ

り、タイマＩＤ＝３において不正に１ヶ月日付をずらし、その後タイマＩＤ＝４で日付を戻していることがわかるため、ファイルアクセス履歴の日時にタイマＩＤ＝３の履歴がついているファイルは不正に日時を偽ろうとした可能性があることがわかる。タイマ設定履歴は内部記憶媒体１５（タイマ設定履歴ファイル４３）に記録されるが、ファイルアクセス履歴は各ファイルと共に大容量記憶媒体１３に記録される。

【００６９】後述するように、ある電子保存装置から他の電子保存装置に対してファイルを移動したり、コピーしたりすることが可能であるが、このような場合にもファイルアクセス履歴の日時に不整合が生じないよう、概念的には図１７に示すようなファイルアクセス履歴を各ファイルに対して記録する。すなわち、図１３に示したように、ファイルアクセス履歴はファイル属性情報ファイル２９に記録される。例えば、図１７において、移動先となる電子保存装置Ｒ０１０－０００１０５５の日時　１９９９０２１７　１０：１３：４３　ＩＤ＝２が移動元の電子保存装置　Ｒ０１０－０００１０３２の日時１９９９０２１７　１０：１０：２１　ＩＤ＝３に相当することがわかるため、移動したファイルに不正が見つかった場合には、電子保存装置をまたいで履歴を辿ることができる。

【００７０】（４）大容量記憶媒体マウント処理

大容量記憶媒体１３が電子保存装置１から取り外し可能な場合には、大容量記憶媒体１３を電子保存装置１に装着した際に、以下に説明する大容量記憶装置マウント処理を実行することにする。その際、媒体の正当性が検証される。

【００７１】図１８は、大容量記憶媒体マウント処理のフローチャートである。電子保存装置１のプロセッサ１１は、大容量記憶媒体１３が電子保存装置１に装着されると、装着された大容量記憶媒体１３がフォーマット済みであるか否かを判定する（Ｓ１２１）。ステップＳ１２１においてフォーマット済みである場合（Ｓ１２１；Ｙｅｓ）はステップＳ１２３に進み、フォーマット済みでない場合（Ｓ１２１；Ｎｏ）は図１９に示す大容量記憶媒体のフォーマット処理が実行される（Ｓ１２２）。

【００７２】すなわち、ステップＳ１２２においては、図１９に示すように、プロセッサ１１が大容量記憶媒体１３の初期化処理を実行し（Ｓ１３１）、乱数を生成する（Ｓ１３２）。プロセッサ１１は、生成した乱数を保存ファイルリスト３２の最初のエントリとして格納する（Ｓ１３３）。その後、プロセッサ１１は、図１０に示したように、保存ファイルリスト３２の改ざん検知保存処理を実行し（Ｓ１３４）、図１８のステップＳ１２３に進む。

【００７３】プロセッサ１１は、図１１に示した処理に従って、保存ファイルリストファイル３１の改ざん検知読み出し処理を実行し（Ｓ１２３）、正常に読み出し処理を実行できた場合（Ｓ１２４；Ｙｅｓ）には大容量記憶媒体マウント処理を正常終了し、読み出し処理に失敗した場合（Ｓ１２４；Ｎｏ）には大容量記憶媒体マウント処理をエラーにより終了する。

【００７４】（５）ファイル読み出し処理

ユーザ側からファイル読み出し要求を受けると、対象ファイルの正当性を検証し、データをユーザに対して送出する。

【００７５】図２０は、ファイル読み出し処理のフローチャートである。電子保存装置１のプロセッサ１１は、ユーザ側からファイル読み出し要求を受けると、大容量記憶媒体１３がマウントされているか否かを判定する（Ｓ１４１）。ここで、大容量記憶媒体１３がマウントされていない場合（Ｓ１４１；Ｎｏ）、ファイル読み出し処理はエラーにより終了する。

【００７６】一方、大容量記憶媒体１３がマウントされている場合（Ｓ１４１；Ｙｅｓ）、プロセッサ１１は、対象ファイル（保存ファイル２５）に関連付けられたファイル属性情報ファイル２９が存在するか否かを判定する（Ｓ１４２）。ファイル属性情報ファイル２９が存在しないと判定した場合（Ｓ１４２；Ｎｏ）、プロセッサ１１は、対象ファイルを読み出してユーザ側に送出する処理を実行し（Ｓ１４６）、ファイル読み出し処理を終了する。これに対し、ファイル属性情報ファイル２９が存在すると判定した場合（Ｓ１４２；Ｙｅｓ）、プロセッサ１１は、図１１に示した処理に従い、対象ファイルの改ざん検知読み出し処理を実行する（Ｓ１４３）。

【００７７】続いて、プロセッサ１１は、改ざん検知読み出し処理で対象ファイルの読み出しに成功したか否かを判定する（Ｓ１４４）。ここで、読み出しに失敗した場合（Ｓ１４４；Ｎｏ）、プロセッサ１１は、ファイル読み出し処理をエラーにより終了する。一方、読み出しに成功した場合（Ｓ１４４；Ｙｅｓ）、プロセッサ１１は、読み出したデータをユーザ側に送出し（Ｓ１４５）、ファイル読み出し処理を正常に終了する。

【００７８】（６）謄本作成処理

「原本」の属性を持つ保存ファイル２５に対し、外部から複製要求を受け取ると、対象ファイルとそれに関連付けられたファイル属性情報ファイル２９をコピーすると共に、新しいファイル属性情報には「謄本」のファイル属性コード２２を付与する。謄本ファイルの作成先が別の電子保存装置の場合には、別の電子保存装置にログインしてファイルを転送する。ログインの方法は、図６を用いて説明したような、ユーザが電子保存装置１にログインする方法と同様である。電子保存装置間でやり取りされるデータの保護についても、ユーザと電子保存装置１との間でやり取りするデータの保護の方法と同様である。データ保存処理と同様に、保存ファイルリスト３２の更新も行われる。なお、ファイル転送先の電子保存装置においては、転送受け入れ処理が行われることにな

る。

【００７９】図２１は、謄本作成処理を示すフローチャートである。電子保存装置１のプロセッサ１１は、図１１に示した処理に従い、謄本を作成する対象となる対象ファイルのファイル属性情報ファイル２９の改ざん検知読み出し処理を実行する（Ｓ１５１）。ここで、改ざん検知読み出し処理に失敗した場合（Ｓ１５２；Ｎｏ）、謄本作成処理をエラーによって終了する。

【００８０】一方、改ざん検知読み出し処理に成功した場合（Ｓ１５２；Ｙｅｓ）、プロセッサ１１は、読み出したファイル属性情報ファイル２９からファイル属性コード２２を取得する（Ｓ１５３）。プロセッサ１１は、取得したファイル属性コード２２が「原本」であるか否かを判定し（Ｓ１５４）、ファイル属性コードが「原本」でない場合（Ｓ１５４；Ｎｏ）、謄本作成処理をエラーによって終了する。

【００８１】ファイル属性コードが「原本」である場合（Ｓ１５４；Ｙｅｓ）、プロセッサ１１は、謄本の作成先が同一装置か否かを判定し（Ｓ１５５）、同一装置であると判定した場合（Ｓ１５５；Ｙｅｓ）には同一装置内での謄本作成処理を実行し（Ｓ１５６）、同一装置ではないと判定した場合（Ｓ１５５；Ｎｏ）には他の装置での謄本作成処理を実行し（Ｓ１５７）、謄本作成処理を終了する。

【００８２】図２２は、図２１のステップＳ１５６において実行される同一装置内での謄本作成処理のフローチャートである。まず、プロセッサ１１は、作成先のファイルが既に存在しているか否かを判定し（Ｓ１６１）、存在している場合（Ｓ１６１；Ｙｅｓ）にはエラーにより同一装置内での謄本作成処理を終了する。換言すれば、図２１に示した謄本作成処理をエラーで終了することになる。

【００８３】一方、作成先のファイルが存在していない場合（Ｓ１６１；Ｎｏ）、プロセッサ１１は、対象ファイルを作成先ファイルにコピーする（Ｓ１６３）。そして、プロセッサ１１は、対象ファイルのファイル属性情報ファイル２９を作成先のファイル属性情報ファイルとしてコピーする（Ｓ１６３）。

【００８４】続いて、プロセッサ１１は、図１１に示した処理に従い、作成先のファイル属性情報ファイル２９の改ざん検知読み出し処理を実行し（Ｓ１６４）、読み出したファイル属性情報２６のファイル属性コード２２を「謄本」に変更する（Ｓ１６５）。

【００８５】プロセッサ１１は、タイマ１７から現在時刻を取得し（Ｓ１６６）、ファイル属性情報２６に謄本作成履歴（アカウント名，現在時刻，タイマＩＤ等）を追加し（Ｓ１６７）、図１０に示した処理に従い、ファイル属性情報２６の改ざん検知保存処理を実行する（Ｓ１６８）。

【００８６】さらに、プロセッサ１１は、保存ファイルリストファイル３１の改ざん検知読み出し処理を実行し（Ｓ１６９）、読み出し処理に失敗した場合（Ｓ１７０；Ｎｏ）、作成先ファイルおよび作成先ファイル属性情報ファイルを削除し（Ｓ１７３）、エラーにより図２２の処理を終了する。すなわち、図２１の謄本作成処理をエラーで終了することになる。

【００８７】一方、読み出し処理に成功した場合（Ｓ１７０；Ｙｅｓ）、プロセッサ１１は、保存ファイルリスト３２に作成先ファイルのエントリを追加し（Ｓ１７１）、図１０に示した処理に従って保存ファイルリスト３２の改ざん検知保存処理を実行して（Ｓ１７２）、図２１の謄本作成処理を正常に終了する。

【００８８】図２３は、図２１のステップＳ１５７において実行される他の装置での謄本作成処理のフローチャートである。プロセッサ１１は、図６に示したような処理に従い、作成先保存装置へのログイン処理を実行する（Ｓ１８１）。ここで、ログイン処理に失敗した場合（Ｓ１８２；Ｎｏ）、プロセッサ１１は図２３の処理をエラーで終了する。すなわち、図２１の処理がエラーで終了することになる。

【００８９】一方、ログイン処理に成功した場合（Ｓ１８２；Ｙｅｓ）、プロセッサ１１は、図１１に示した処理に従い、対象ファイルの改ざん検知読み出し処理を実行し（Ｓ１８３）、読み出しデータを作成先保存装置に謄本作成モードで転送する（Ｓ１８４）。

【００９０】続いて、プロセッサ１１は、図１１に示した処理に従い、対象ファイルのファイル属性情報ファイル２９の改ざん検知読み出し処理を実行する（Ｓ１８５）。そして、プロセッサ１１は、タイマ１７から現在時刻を取得し（Ｓ１８６）、ファイル属性情報２６に謄本作成履歴を追加する（Ｓ１８７）。

【００９１】そして、プロセッサ１１は、ファイル属性情報２６を作成先保存装置に謄本作成モードで転送し（Ｓ１８８）、転送が成功した場合には（Ｓ１８９；Ｙｅｓ）、作成先保存装置からログアウトし（Ｓ１９０）、図２１に示す謄本作成処理を終了する。一方、転送に失敗した場合（Ｓ１８９；Ｎｏ）、図２３の処理をエラーで終了する。すなわち、図２１の謄本作成処理もエラーで終了ということになる。

【００９２】図２４は、図２３に示す他の装置での謄本作成処理が実行された場合に、他の装置、即ち図２３に示した作成先保存装置で行われる転送受け入れ処理（謄本作成モード）を示すフローチャートである。作成先保存装置は、転送先ファイルが既に存在しているか否かを判定し（Ｓ１９１）、転送先ファイルが既に存在している場合（Ｓ１９１；Ｙｅｓ）にはエラーで図２４の処理を終了する。この場合、図２１の謄本作成処理もエラーで終了ということになる。

【００９３】また、作成先保存装置は、転送先ファイルが存在しないと判定した場合（Ｓ１９１；Ｎｏ），図１

1に示した処理に従い、保存ファイルリストファイル31の改ざん検知読み出し処理を実行する（S192）。ここで、改ざん検知読み出し処理に失敗した場合（S193；No）、エラーにより図24の処理を終了する。一方、読み出しに成功した場合（S193；Yes）、作成先保存装置は、図10に示した処理に従い、受け取ったデータの改ざん検知保存処理を実行する（S194）。

【0094】続いて、作成先保存装置は、受け取ったファイル属性情報26のファイル属性コード22を「謄本」に変更し（S195）、ファイル属性情報26に謄本作成履歴を追加して（S196）、図10に示した処理に従ってファイル属性情報26の改ざん検知保存処理を実行する（S197）。

【0095】その後、作成先保存装置は、保存ファイルリスト32に作成した謄本ファイルのエントリを追加し（S198）、図10に示した処理に従い、保存ファイルリスト32の改ざん検知保存処理を実行し（S199）、図24の処理を終了する。

【0096】（7）バックアップ作成処理

「仮原本」，「原本」，「謄本」の属性を持つファイルに対して外部からバックアップ作成要求を受け取ると、対象ファイルと、それに関連付けられたファイル属性情報ファイルをコピーし、新しいファイル属性ファイルには元のファイル属性コードに対応する「バックアップ仮原本」，「バックアップ原本」，「バックアップ謄本」というファイル属性コードをつけることにする。バックアップファイルの作成先が別の電子保存装置の場合には、その別の電子保存装置にログインしてファイルを転送する。データ保存処理と同様に、保存ファイルリストの更新も行う。なお、ファイル転送先の電子保存装置では、転送受け入れ処理が行われることになる。

【0097】図25は、バックアップ作成処理のフローチャートである。電子保存装置1のプロセッサ11は、バックアップの作成対象となる対象ファイルのファイル属性情報ファイル29の改ざん検知読み出し処理を実行する（S201）。ここで、改ざん検知読み出し処理による読み出しに失敗した場合（S202；No）、エラーによりバックアップ作成処理を終了する。

【0098】一方、読み出しに成功した場合（S202；Yes）、読み出したファイル属性情報ファイル29からファイル属性コード22を取得する（S203）。そして、プロセッサ11は、バックアップ作成先が同一装置か否かを判定し（S204）、同一装置と判定した場合（S204；Yes）には同一装置内でのバックアップ作成処理を実行し（S205）、同一装置ではないと判定した場合（S204；No）には他の装置でのバックアップ作成処理を実行し（S206）、バックアップ作成処理を終了する。

【0099】図26は、図25のステップS205において実行される同一装置内でのバックアップ作成処理のフローチャートである。プロセッサ11は、作成先のファイルが既に存在するか否かを判定し（S210）、存在する場合（S210；Yes）にはエラーとして図25および図26に示すバックアップ作成処理を終了する。一方、作成先のファイルが存在しない場合（S210；No）には対象ファイルを作成先ファイルにコピーする（S211）。

【0100】続いて、プロセッサ11は、対象ファイルのファイル属性情報ファイル29を作成先のファイル属性情報ファイルとしてコピーする（S212）。プロセッサ11は、さらに、図11に示した処理に従い、作成先のファイル属性情報ファイル29の改ざん検知読み出し処理を実行し（S213）、ファイル属性コード22を変更する処理を実行する（S214）。

【0101】具体的には、ファイル属性コードが「仮原本」の場合は「バックアップ仮原本」に変更し、「原本」の場合は「バックアップ原本」に変更し、「謄本」の場合は「バックアップ謄本」に変更する。

【0102】そして、プロセッサ11は、タイマ17から現在時刻を取得し（S215）、ファイル属性情報26にバックアップ作成履歴（アカウント名，現在時刻，タイマID等）を追加した後（S216）、図10に示した処理に従い、ファイル属性情報26の改ざん検知保存処理を実行する（S217）。

【0103】続いて、プロセッサ11は、図11に示した処理に従い、保存ファイルリストファイル31の改ざん検知読み出し処理を実行し（S218）、読み出しに成功した場合（S219；Yes）、保存ファイルリスト32に作成先ファイルのエントリを追加し（S220）、図10に示した処理に従って保存ファイルリスト32の改ざん検知保存処理を実行して（S221）、図26の処理を終了する。

【0104】一方、保存ファイルリストファイル31の改ざん検知読み出し処理に失敗した場合（S219；No）、作成先ファイルおよび作成先ファイル属性情報ファイルを削除する処理を実行し（S222）、エラーとして図25および図26の処理を終了する。

【0105】図27は、図25のステップS206において実行される他の装置でのバックアップ作成処理のフローチャートである。電子保存装置1のプロセッサ11は、図6に示したようにして、作成先保存装置へのログイン処理を実行する（S231）。ここで、ログイン処理に成功しなかった場合（S232；No）は、エラーにより図25および図27の処理を終了し、ログイン処理に成功した場合（S232；Yes）は、図11に示した処理に従って対象ファイルの改ざん検知読み出し処理を実行する（S233）。

【0106】続いて、プロセッサ11は、読み出しデータを作成先保存装置にバックアップ作成モードで転送し

（Ｓ２３４）、図１１に示した処理に従い、対象ファイルのファイル属性情報ファイル２９の改ざん検知読み出し処理を実行する（Ｓ２３５）。

【０１０７】そして、プロセッサ１１は、タイマ１７から現在時刻を取得し（Ｓ２３６）、ファイル属性情報２６に謄本作成履歴を追加する（Ｓ２３７）。そして、プロセッサ１１は、ファイル属性情報２６を作成先保存装置にバックアップ作成モードで転送し（Ｓ２３８）、転送が成功した場合（Ｓ２３９；Ｙｅｓ）には作成先保存装置からのログアウト処理を実行して（Ｓ２４０）、図２７に示す処理を正常に終了する。一方、転送に失敗した場合（Ｓ２３９）、エラーにより図２５および図２７に示す処理が終了する。

【０１０８】図２８は、図２７に示す他の装置でのバックアップ作成処理が実行された場合に、他の装置、即ち図２７に示した作成先保存装置で行われる転送受け入れ処理（バックアップ作成モード）を示すフローチャートである。作成先保存装置は、転送先ファイルが既に存在しているか否かを判定し（Ｓ２４１）、転送先ファイルが既に存在している場合（Ｓ２４１；Ｙｅｓ）にはエラーで図２８の処理を終了する。この場合、図２５のバックアップ作成処理もエラーで終了ということになる。

【０１０９】また、作成先保存装置は、転送先ファイルが存在しないと判定した場合（Ｓ２４１；Ｎｏ），図１１に示した処理に従って、保存ファイルリストファイル３１の改ざん検知読み出し処理を実行する（Ｓ２４２）。ここで、改ざん検知読み出し処理に失敗した場合（Ｓ２４３；Ｎｏ）、エラーにより図２８の処理を終了する。一方、読み出しに成功した場合（Ｓ２４３；Ｙｅｓ）、作成先保存装置は、図１０に示した処理に従って、受け取ったデータの改ざん検知保存処理を実行する（Ｓ２４４）。

【０１１０】続いて、作成先保存装置は、受け取ったファイル属性情報２６のファイル属性コード２２を値に応じて「バックアップ」に変更し（Ｓ２４５）、ファイル属性情報２６にバックアップ作成履歴を追加して（Ｓ２４６）、図１０に示した処理に従ってファイル属性情報２６の改ざん検知保存処理を実行する（Ｓ２４７）。

【０１１１】その後、作成先保存装置は、保存ファイルリスト３２に作成したバックアップファイルのエントリを追加し（Ｓ２４８）、図１０に示した処理に従って、保存ファイルリスト３２の改ざん検知保存処理を実行し（Ｓ２４９）、図２８の処理を終了する。

【０１１２】（８）ファイル移動処理

同一の電子保存装置１内または別の電子保存装置１へファイルを移動する際には、このファイル移動処理が実行される。ファイルの移動先が別の電子保存装置１の場合、移動先の電子保存装置１においては、転送受け入れ処理が実行される。

【０１１３】図２９は、ファイル移動処理を示すフローチャートである。電子保存装置１のプロセッサ１１は、ファイルの移動処理の実行が指定されると、移動先が同一装置内であるか否かを判定し（Ｓ２５１）、移動先が同一装置内であると判定した場合（Ｓ２５１；Ｙｅｓ）、作成先のファイルが既に存在しているか否かを判定する（Ｓ２５２）。

【０１１４】ステップＳ２５２において、作成先のファイルが既に存在していると判定した場合（Ｓ２５２；Ｙｅｓ）、プロセッサ１１は、エラーとしてファイル移動処理を終了する。一方、作成先のファイルが存在していないと判定した場合（Ｓ２５２；Ｎｏ）、プロセッサ１１は、図１１に示した処理に基づいて、保存ファイルリストファイル３１の改ざん検知読み出し処理を実行する（Ｓ２５３）。そして、プロセッサ１１は、改ざん検知読み出し処理に失敗した場合（Ｓ２５４；Ｎｏ）、エラーとしてファイル移動処理を終了する。一方、改ざん検知読み出し処理が成功した場合（Ｓ２５４；Ｙｅｓ）、対象ファイル（保存ファイル２５）を移動先ファイルに移動する（Ｓ２５５）。

【０１１５】また、プロセッサ１１は、対象ファイルにファイル属性情報ファイル２９が存在しているか否かを判定し（Ｓ２５６）、存在していないと判定した場合（Ｓ２５６；Ｎｏ）にはステップＳ２５８に進み、存在していると判定した場合（Ｓ２５６；Ｙｅｓ）には、ファイル属性情報ファイル２９を移動先のファイル属性情報ファイルとして移動する（Ｓ２５７）。

【０１１６】そして、プロセッサ１１は、保存ファイルリスト３２内の移動したファイルのエントリを更新し（Ｓ２５８）、図１０に示した処理に従って保存ファイルリスト３２の改ざん検知保存処理を実行し（Ｓ２５９）、ファイル移動処理を終了する。

【０１１７】さらに、プロセッサ１１は、ステップＳ２５１において移動先が同一装置内ではないと判定した場合（Ｓ２５１；Ｎｏ）、他の装置へのファイル移動処理を実行する（Ｓ２６０）。

【０１１８】図３０は、図２９のステップＳ２６０において実行される他の装置へのファイル移動処理を示すフローチャートである。電子保存装置１のプロセッサ１１は、図１１に示した処理に従い、保存ファイルリストファイル３１の改ざん検知読み出し処理を実行する（Ｓ２６１）。プロセッサ１１は、改ざん検知読み出し処理に失敗した場合に（Ｓ２６２；Ｎｏ）、エラーとして図３０および図２９のファイル移動処理を終了し、改ざん検知読み出し処理に成功した場合（Ｓ２６２；Ｙｅｓ）、移動先保存装置へのログイン処理を実行する（Ｓ２６３）。

【０１１９】プロセッサ１１は、ログイン処理に失敗した場合（Ｓ２６４；Ｎｏ）、エラーとして図３０および図２９のファイル移動処理を終了し、ログイン処理に成功した場合（Ｓ２６４；Ｙｅｓ）、図１１に示した処理

に従って、移動するファイルとして指定された保存ファイル２５、即ち対象ファイルの改ざん検知読み出し処理を実行し（Ｓ２６５）、読み出しデータを移動先保存装置に移動モードで転送する（Ｓ２６６）。プロセッサ１１は、転送に失敗した場合（Ｓ２６７；Ｎｏ）、エラーとして図３０および図２９のファイル移動処理を終了し、転送に成功した場合（Ｓ２６７；Ｙｅｓ）、対象ファイルにファイル属性情報ファイル２９が存在しているか否かを判定する（Ｓ２６８）。ファイル属性情報ファイル２９が存在していないと判定した場合は（Ｓ２６８；Ｎｏ）、ステップＳ２７４に進む。

【０１２０】一方、ファイル属性情報ファイル２９が存在していると判定した場合（Ｓ２６８；Ｙｅｓ）、プロセッサ１１は、図１１に示した処理に従って、ファイル属性情報ファイル２９の改ざん検知読み出し処理を実行する（Ｓ２６９）。そして、プロセッサ１１は、タイマ１７から現在時刻を取得し（Ｓ２７０）、ファイル属性情報２６にファイル移動履歴を追加する（Ｓ２７１）。その後、プロセッサ１１は、ファイル属性情報２６を移動先保存装置に移動モードで転送する（Ｓ２７２）。

【０１２１】続いて、プロセッサ１１は、転送に失敗した場合（Ｓ２７３；Ｎｏ）、エラーとして図３０および図２９のファイル移動処理を終了し、転送に成功した場合（Ｓ２７３；Ｙｅｓ）、対象ファイルの削除（Ｓ２７４），対象ファイルのファイル属性情報ファイル２９の削除（Ｓ２７５），保存ファイルリスト３２内に存在する移動したファイルのエントリの削除（Ｓ２７６），図１０に示した処理に基づく保存ファイルリスト３２の改ざん検知保存処理（Ｓ２７７）および作成先保存装置からのログアウト処理（Ｓ２７８）を順次実行して図３０および図２９のファイル移動処理を終了する。

【０１２２】図３１は、図３０に示す他の装置へのファイル移動処理が実行された場合に、他の装置、即ち図３０に示した移動先保存装置で行われる転送受け入れ処理（移動モード）を示すフローチャートである。移動先保存装置は、転送先ファイルが既に存在しているか否かを判定し（Ｓ２８１）、転送先ファイルが存在していると判定した場合（Ｓ２８１；Ｙｅｓ）、エラーとして転送受け入れ処理を終了する。

【０１２３】一方、転送先ファイルが存在していないと判定した場合（Ｓ２８１；Ｎｏ）、移動先保存装置は、図１１に示した処理に従い、保存ファイルリストファイル３１の改ざん検知読み出し処理を実行する（Ｓ２８２）。移動先保存装置は、改ざん検知読み出し処理に失敗した場合（Ｓ２８３；Ｎｏ）、エラーとして転送受け入れ処理を終了し、改ざん検知読み出し処理に成功した場合（Ｓ２８３；Ｙｅｓ）、図１０に示した処理に従って、受け取ったデータの改ざん検知保存処理を実行する（Ｓ２８４）。

【０１２４】さらに、移動先保存装置は、ファイル属性情報２６を受け取ったか否かを判定し（Ｓ２８５）、受け取っていない場合には（Ｓ２８５；Ｎｏ）そのまま処理を終了し、受け取った場合には（Ｓ２８５；Ｙｅｓ）ファイル属性情報２６にファイル移動履歴を追加する（Ｓ２８６）。

【０１２５】そして、移動先保存装置は、図１０に示した処理に従ってファイル属性情報２６の改ざん検知保存処理を実行し（Ｓ２８７）、保存ファイルリスト３２に受け取ったファイルのエントリを追加し（Ｓ２８８）、図１０に示した処理に従って保存ファイルリスト３２の改ざん検知保存処理を実行して（Ｓ２８９）、転送受け入れ処理を終了する。

【０１２６】（９）ファイル削除処理

保存ファイル２５を削除するための処理である。しかし、「原本」のファイル属性コード２２を有する保存ファイル２５については証拠隠滅を防ぐために削除は禁止される。

【０１２７】図３２は、ファイル削除処理を示すフローチャートである。電子保存装置１のプロセッサ１１は、ファイルの削除が指定されると、大容量記憶媒体１３がマウントされているか否かを判定し（Ｓ２９１）、マウントされていないと判定した場合（Ｓ２９１；Ｎｏ）、エラーとしてファイル削除処理を終了する。一方、マウントされていると判定した場合（Ｓ２９１；Ｙｅｓ）、削除が指定された保存ファイル２５、即ち対象ファイルに対応するファイル属性情報ファイル２９が存在するか否かを判定する（Ｓ２９２）。

【０１２８】プロセッサ１１は、ファイル属性情報ファイル２９が存在しないと判定した場合（Ｓ２９２；Ｎｏ）、対象ファイルを削除し（Ｓ３０２）、ファイル削除処理を終了する。一方、ファイル属性情報ファイル２９が存在すると判定した場合（Ｓ２９２；Ｙｅｓ）、図１１に示した処理に従って、対象ファイルに対応するファイル属性情報ファイル２９の改ざん検知読み出し処理を実行する（Ｓ２９３）。

【０１２９】そして、プロセッサ１１は、改ざん検知読み出し処理に失敗した場合（Ｓ２９４；Ｎｏ）、エラーとしてファイル削除処理を終了し、改ざん検知読み出し処理に成功した場合（Ｓ２９４；Ｙｅｓ）、ファイル属性情報２６に含まれるファイル属性コード２２が「原本」であるか否かを判定する（Ｓ２９５）。

【０１３０】ファイル属性コード２２が「原本」であると判定した場合（Ｓ２９５；Ｙｅｓ）、原本の削除は禁止されているため、プロセッサ１１はエラーとしてファイル削除処理を終了する。一方、「原本」ではないと判定した場合（Ｓ２９５；Ｎｏ）、プロセッサ１１は、対象ファイルを削除し（Ｓ２９６）、さらに、ファイル属性情報ファイル２９を削除する（Ｓ２９７）。

【０１３１】続いて、プロセッサ１１は、図１１に示した処理に従って、保存ファイルリストファイル３１の改

ざん検知読み出し処理を実行する（Ｓ２９８）。プロセッサ１１は、改ざん検知読み出し処理に失敗した場合（Ｓ２９９；Ｎｏ）、エラーとしてファイル削除処理を終了し、改ざん検知読み出し処理に成功した場合（Ｓ２９９；Ｙｅｓ）、保存ファイルリスト３２から対象ファイルのエントリを削除し（Ｓ３００）、図１０に示した処理に従って保存ファイルリスト３２の改ざん検知保存処理を実行して（Ｓ３０１）、ファイル削除処理を終了する。

【０１３２】（１０）ファイル属性コード変更処理

データ保存処理において、「仮原本」の属性を持つファイルを保存することが可能であるが、この「仮原本」ファイルは単純にファイル属性コード２２を「原本」に変更することが可能なものである。また、「謄本」，「バックアップ仮原本」，「バックアップ原本」および「バックアップ謄本」の属性を持つファイルは、それぞれファイル属性コード２２を変更することで元のファイルを復旧するために利用することができる。復旧すると、ファイル属性コードは図３３に示すようになる。

【０１３３】ファイル属性コード２２の変更は、ファイルアクセス履歴として記録される。このファイル属性コード変更処理は、外部からのファイル属性コード２２の変更要求と共に、新しいファイル属性コード２２を受け取ることによって実行される。

【０１３４】図３４は、ファイル属性コード変更処理を示すフローチャートである。電子保存装置１のプロセッサ１１は、ファイル属性コード変更処理の指示があると、大容量記憶媒体１３がマウントされているか否かを判定する（Ｓ３１０）。プロセッサ１１は、大容量記憶媒体１３がマウントされていないと判定した場合（Ｓ３１０；Ｎｏ）、エラーとしてファイル属性コード変更処理を終了し、大容量記憶媒体１３がマウントされていると判定した場合（Ｓ３１０；Ｙｅｓ）、変更対象の保存ファイル２５、即ち対象ファイルに対応するファイル属性情報ファイル２９が存在しているか否かを判定する（Ｓ３１１）。

【０１３５】プロセッサ１１は、ファイル属性情報ファイル２９が存在しないと判定した場合（Ｓ３１１；Ｎｏ）、エラーとしてファイル属性コード変更処理を終了し、存在すると判定した場合（Ｓ３１１；Ｙｅｓ）、図１１に示す処理に従ってファイル属性情報ファイル２９の改ざん検知読み出し処理を実行する（Ｓ３１２）。プロセッサ１１は、改ざん検知読み出し処理に失敗した場合（Ｓ３１３；Ｎｏ）、エラーとしてファイル属性コード変更処理を終了し、改ざん検知読み出し処理に成功した場合（Ｓ３１３；Ｙｅｓ）、指定された新ファイル属性コードに応じたコード変更処理を実行する（Ｓ３１４）。

【０１３６】図３５（ａ）～図３５（ｃ）は、図３４のステップＳ３１４において実行されるコード変更処理のフローチャートである。図３５（ａ）は新ファイル属性コードとして「仮原本」が指定された場合であり、プロセッサ１１は、現在のファイル属性コード２２が「バックアップ仮原本」であるか否かを判定する（Ｓ３３１）。現在のファイル属性コード２２が「バックアップ仮原本」ではない場合（Ｓ３３１；Ｎｏ）、エラーとして図３５および図３４のファイル属性コード変更処理を終了する。一方、現在のファイル属性コード２２が「バックアップ仮原本」である場合（Ｓ３３１；Ｙｅｓ）、ファイル属性情報２６のファイル属性コード２２を「仮原本」に変更する処理を実行する（Ｓ３３２）。

【０１３７】また、図３５（ｂ）は新ファイル属性コードとして「原本」が指定された場合であり、プロセッサ１１は、現在のファイル属性コード２２が「バックアップ原本」または「仮原本」であるか否かを判定する（Ｓ３４１）。現在のファイル属性コード２２が「バックアップ原本」または「仮原本」ではない場合（Ｓ３４１；Ｎｏ）、エラーとして図３５および図３４のファイル属性コード変更処理を終了する。一方、現在のファイル属性コード２２が「バックアップ原本」または「仮原本」である場合（Ｓ３４１；Ｙｅｓ）、ファイル属性情報２６のファイル属性コード２２を「原本」に変更する処理を実行する（Ｓ３４２）。

【０１３８】さらに、図３５（ｃ）は新ファイル属性コードとして「謄本」が指定された場合であり、プロセッサ１１は、現在のファイル属性コード２２が「バックアップ謄本」であるか否かを判定する（Ｓ３５１）。現在のファイル属性コード２２が「バックアップ謄本」ではない場合（Ｓ３５１；Ｎｏ）、エラーとして図３５および図３４のファイル属性コード変更処理を終了する。一方、現在のファイル属性コード２２が「バックアップ謄本」である場合（Ｓ３５１；Ｙｅｓ）、ファイル属性情報２６のファイル属性コード２２を「謄本」に変更する処理を実行する（Ｓ３５２）。

【０１３９】図３４のフローチャートの説明に戻り、プロセッサ１１は、図３５を用いて説明したステップＳ３１４においてコード変更処理を行った後、タイマ１７から現在時刻を取得し（Ｓ３１５）、ファイル属性情報２６にファイル属性コード変更履歴を追加する（Ｓ３１６）。

【０１４０】続いて、プロセッサ１１は、図１０に示した処理に従ってファイル属性情報２６の改ざん検知保存処理を行い（Ｓ３１７）、図１１に示した処理に従って保存ファイルリストファイル３１の改ざん検知読み出し処理を実行する（Ｓ３１８）。そして、プロセッサ１１は、改ざん検知読み出し処理に失敗した場合（Ｓ３１９；Ｎｏ）、エラーとしてファイル属性コード変更処理を終了する。一方、改ざん検知読み出し処理に成功した場合（Ｓ３１９；Ｙｅｓ）、プロセッサ１１は、保存ファイルリスト３２の対象ファイルのエントリについて内

容を更新し（Ｓ３２０）、図１０に示した処理に従って保存ファイルリスト３２の改ざん検知保存処理を実行して（Ｓ３２１）、ファイル属性コード変更処理を終了する。

【０１４１】（１１）ファイル追記処理

「原本」や「仮原本」のファイル属性コード２２を持つファイルに対しては、編集は許可しないが追記は可能とする。追記のみを許可することにより、以前のデータが失われず、電子データの編集履歴がわかるため、その証明力も高まることになる。また、「謄本」およびバックアップのファイルについては追記も編集も許可しない。これは、データの訂正や修正は原本に対して施すべきものであって、コピーである謄本に施すべきものではないという考えに基づくものである。なお、ファイルの最終更新日時が変更されるため、データ保存処理と同様に保存ファイルリスト３２についても更新されることになる。

【０１４２】図３６は、ファイル追記処理を示すフローチャートである。電子保存装置１のプロセッサ１１は、大容量記憶媒体１３がマウントされているか否かを判定し（Ｓ３６１）、マウントされていない場合（Ｓ３６１；Ｎｏ）、エラーとしてファイル追記処理を終了する。

【０１４３】一方、大容量記憶媒体１３がマウントされていると判定した場合（Ｓ３６１；Ｙｅｓ）、プロセッサ１１は、追記処理の対象となる保存ファイル２５、即ち対象ファイルに対応するファイル属性情報ファイル２９が存在するか否かを判定する（Ｓ３６２）。プロセッサ１１は、ファイル属性情報ファイル２９が存在しないと判定した場合（Ｓ３６２；Ｎｏ）、対象ファイルにデータを追記する処理を実行し（Ｓ３７４）、ファイル追記処理を終了する。一方、ファイル属性情報ファイル２９が存在すると判定した場合（Ｓ３６２；Ｙｅｓ）、プロセッサ１１は、図１１に示した処理に従い、ファイル属性情報ファイル２９の改ざん検知読み出し処理を実行する（Ｓ３６３）。

【０１４４】そして、プロセッサ１１は、改ざん検知読み出し処理に失敗した場合（Ｓ３６４；Ｎｏ）、エラーとしてファイル追記処理を終了し、改ざん検知読み出し処理に成功した場合（Ｓ３６４；Ｙｅｓ）、ファイル属性コード２２が「原本」または「仮原本」であるか否かを判定する（Ｓ３６５）。「原本」または「仮原本」でない場合（Ｓ３６５；Ｎｏ）、エラーとしてファイル追記処理を終了し、「原本」または「仮原本」である場合（Ｓ３６５；Ｙｅｓ）、図１１に示した処理に従って、対象ファイルの改ざん検知読み出し処理を実行する（Ｓ３６６）。

【０１４５】プロセッサ１１は、改ざん検知読み出し処理に失敗した場合（Ｓ３６７；Ｎｏ）、エラーとしてファイル追記処理を終了し、改ざん検知読み出し処理に成功した場合（Ｓ３６７；Ｙｅｓ）、図１１に示した処理に従い、保存ファイルリストファイル３１の改ざん検知読み出し処理を実行する（Ｓ３６８）。

【０１４６】プロセッサ１１は、改ざん検知読み出し処理に失敗した場合（Ｓ３６９；Ｎｏ）、エラーとしてファイル追記処理を終了し、改ざん検知読み出し処理に成功した場合（Ｓ３６９；Ｙｅｓ）、読み出しデータに追記データを追加する処理を実行する（Ｓ３７０）。

【０１４７】そして、プロセッサ１１は、図１０に示した処理に従って追記済みデータの改ざん検知保存処理を実行し（Ｓ３７１）、保存ファイルリスト３２中の対象ファイルのエントリを更新し（Ｓ３７２）、さらに、図１０に示した処理に従って保存ファイルリスト３２の改ざん検知保存処理を実行して（Ｓ３７３）、ファイル追記処理を終了する。

【０１４８】（１２）ファイル編集処理

「仮原本」や「原本」ファイルについては修正履歴を残すことで証明力を高めるため、これらのファイルに対する編集要求については拒否するものとする。また、「謄本」ファイルやバックアップファイルは、本来編集すべき対象ではないため、これらのファイルに対する編集要求についても拒否することにする。したがって、ここでは「一般」ファイルのみ編集可能とする。

【０１４９】図３７は、ファイル編集処理を示すフローチャートである。電子保存装置１のプロセッサ１１は、大容量記憶媒体１３がマウントされているか否かを判定し（Ｓ３８１）、マウントされていない場合（Ｓ３８１；Ｎｏ）、エラーとしてファイル編集処理を終了する。

【０１５０】一方、大容量記憶媒体１３がマウントされていると判定した場合（Ｓ３８１；Ｙｅｓ）、プロセッサ１１は、編集対象として指定された保存ファイル２５、即ち対象ファイルにファイル属性情報ファイル２９が存在しているか否かを判定する（Ｓ３８２）。ファイル属性情報ファイル２９が存在している場合（Ｓ３８２；Ｙｅｓ）、そのファイルは「一般」ファイルではないため、エラーとしてファイル編集処理を終了する。一方、ファイル属性情報ファイル２９が存在していない場合（Ｓ３８２；Ｎｏ）、プロセッサ１１は、対象ファイルの編集処理を実行し（Ｓ３８３）、ファイル編集処理を終了する。

【０１５１】このように、本実施の形態に係る原本性保証電子保存方法によれば、電子データの改ざんを防止することに加えて、紙の原本が有する性質を電子情報に持たせることを可能とすることにより、電子情報の証明力を高めることができる。

【０１５２】以上説明した本実施の形態に係る原本性保証電子保存方法は、予め用意されたプログラムを図１に示したような電子保存装置１（コンピュータ）で実行することによって実現することが可能である。換言すれ

ば、このようなプログラムを電子保存装置1（コンピュータ）で実行することにより、例えばファイル管理システムと同じローカルネットワーク上に存在する原本性保証サーバを実現することが可能となる。

【0153】また、上記プログラムを、図1に示した電子保存装置1に予めインストールして提供することにしても良いし、フロッピーディスク，CD-ROM，MO，DVD等のコンピュータで読み取り可能な記録媒体に記録して提供することにしても良い。加えて、上記プログラムを、ネットワークや放送波等を介して提供することもできる。

【0154】

【発明の効果】以上説明したように、本発明の原本性保証電子保存方法（請求項1）によれば、電子データを保存する際に、少なくとも原本の電子データとその他の電子データとを識別可能な状態で保存し、原本の電子データに対するアクセス制御のレベルおよびその他の電子データに対するアクセス制御のレベルを制御するため、紙の原本が有する性質を電子情報に持たせ、電子情報の証明力を高めることが可能となる。

【0155】また、本発明の原本性保証電子保存方法（請求項2）によれば、電子データが対応する属性情報と共に保存され、属性情報がユーザによる編集入力を行えないように管理されており、原本の電子データに対し、属性情報として原本であることを示す属性コードを付与するため、紙の原本が有する性質を電子情報に持たせることが可能となる。

【0156】また、本発明の原本性保証電子保存方法（請求項3）によれば、さらに、原本の電子データに対する修正履歴を記録することにしたため、電子情報の証明力を高めることが可能となる。

【0157】また、本発明の原本性保証電子保存方法（請求項4）によれば、さらに、原本の電子データに対する削除処理の実行を禁止することにしたため、電子情報の証明力を高めることが可能となる。

【0158】また、本発明の原本性保証電子保存方法（請求項5）によれば、さらに、原本の電子データの複製を生成し、生成した複製を原本に対する謄本として管理するようしたため、紙が有する性質を電子情報に持たせることができる。

【0159】また、本発明の原本性保証電子保存方法（請求項6）によれば、さらに、原本の電子データの作成もしくは修正した順番または時刻に関する情報を、外部から変更できないようにするか、または変更されても変更された事実を検出可能な状態で、原本の電子データと共に保存するため、電子情報の証明力を高めることが可能となる。

【0160】また、本発明の原本性保証電子保存方法（請求項7）によれば、さらに、電子データの移動が要求された場合に、電子データを対応する属性情報と共に移動させることにしたため、移動先においても移動元と同様に、電子データに対するアクセス制御のレベルを制御することが可能となる。

【0161】また、本発明の原本性保証電子保存方法（請求項8）によれば、さらに、原本または謄本の電子データおよび対応する属性情報にメッセージ認証子を付与して保存し、電子データがアクセスされた場合に、メッセージ認証子を用いて電子データに対する改ざんを検出するため、電子情報の証明力を高めることが可能となる。

【0162】また、本発明の原本性保証電子保存方法（請求項9）によれば、さらに、第1の保存装置に存在する電子データの複製を第2の保存装置に生成するための要求または第1の保存装置に存在する電子データを第2の保存装置に移動させるための要求があった場合に、第1の保存装置が、電子データおよび対応する属性情報のそれぞれに付与されたメッセージ認証子を検証した後、メッセージ認証子を除いた電子データおよび対応する属性情報を第2の保存装置に転送し、第2の保存装置が、電子データおよび対応する属性情報を受け取り、処理内容に応じて属性情報を変更し、電子データおよび対応する属性情報に対してメッセージ認証子を付与して保存するため、紙の原本が有する性質を電子情報に持たせ、電子情報の証明力を高めることが可能となる。

【0163】さらに、本発明のコンピュータ読み取り可能な記録媒体（請求項10）によれば、請求項1～9のいずれか一つに記載の原本性保証電子保存方法をコンピュータに実行させるためのプログラムを記録したことにより、このプログラムをコンピュータに実行させることにより、例えばユーザサイトに設置可能な原本性保証機能を有する認証サーバを実現することが可能となる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る原本性保証電子保存方法を実行する電子保存装置のブロック構成図である。

【図2】本発明の実施の形態に係るユーザ登録処理を示すフローチャートであり、（a）はクライアント側で実行されるユーザ登録処理を、（b）は電子保存装置側で実行されるユーザ登録処理をそれぞれ示している。

【図3】図2（b）のステップS28で用いられるアカウント管理ファイルの内容を示す説明図である。

【図4】図3に示す認証鍵情報の内容を示す説明図である。

【図5】図3中に示す日時情報の内容を示す説明図である。

【図6】本発明の実施の形態に係る電子保存装置へのログイン処理を示すフローチャートであり、（a）はクライアント側で実行されるログイン処理を、（b）は電子保存装置側で実行されるログイン処理をそれぞれ示している。

【図7】図6（a）のステップS35および図6（b）

のステップS41において実行される相互認証処理のフローチャートであり、(a)はクライアント側で実行される相互認証処理を、(b)は電子保存装置側で実行される相互認証処理をそれぞれ示している。

【図8】本発明の実施の形態に係る電子データ保存処理を示すフローチャートである。

【図9】図8に示す電子データ保存処理において、原本データを保存する際の処理の説明図である。

【図10】本発明の実施の形態に係る改ざん検知保存処理を示すフローチャートである。

【図11】本発明の実施の形態に係る改ざん検知読み出し処理を示すフローチャートである。

【図12】図9に示す保存ファイルの説明図である。

【図13】図9に示すファイル属性情報ファイルの説明図である。

【図14】図9に示す保存ファイルリストファイルの説明図である。

【図15】図9に示すタイマ設定履歴ファイルの説明図である。

【図16】図15に示すタイマ設定履歴ファイル中のタイマ設定履歴の説明図である。

【図17】図13に示すファイル属性情報ファイル中のアクセス履歴の説明図である。

【図18】本発明の実施の形態に係る大容量記憶媒体マウント処理のフローチャートである。

【図19】図19のステップS122で実行される大容量記憶媒体のフォーマット処理を示すフローチャートである。

【図20】本発明の実施の形態に係るファイル読み出し処理のフローチャートである。

【図21】本発明の実施の形態に係る謄本作成処理を示すフローチャートである。

【図22】図21のステップS156において実行される同一装置内での謄本作成処理のフローチャートである。

【図23】図21のステップS157において実行される他の装置での謄本作成処理のフローチャートである。

【図24】図23に示す他の装置での謄本作成処理が実行された場合に、他の装置で行われる転送受け入れ処理(謄本作成モード)を示すフローチャートである。

【図25】本発明の実施の形態に係るバックアップ作成処理のフローチャートである。

【図26】図25のステップS205において実行される同一装置内でのバックアップ作成処理のフローチャートである。

【図27】図25のステップS206において実行される他の装置でのバックアップ作成処理のフローチャートである。

【図28】図27に示す他の装置でのバックアップ作成処理が実行された場合に、他の装置で行われる転送受け入れ処理(バックアップ作成モード)を示すフローチャートである。

【図29】本発明の実施の形態に係るファイル移動処理を示すフローチャートである。

【図30】図29のステップS260において実行される他の装置へのファイル移動処理を示すフローチャートである。

【図31】図30に示す他の装置へのファイル移動処理が実行された場合に、他の装置で行われる転送受け入れ処理(移動モード)を示すフローチャートである。

【図32】本発明の実施の形態に係るファイル削除処理を示すフローチャートである。

【図33】本発明の実施の形態に係るファイル属性コード変更処理の説明図である。

【図34】本発明の実施の形態に係るファイル属性コード変更処理を示すフローチャートである。

【図35】図34のステップS314において実行されるコード変更処理のフローチャートである。

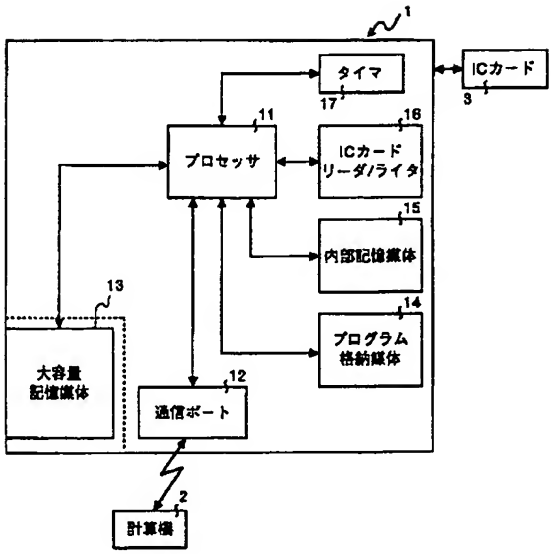
【図36】本発明の実施の形態に係るファイル追記処理を示すフローチャートである。

【図37】本発明の実施の形態に係るファイル編集処理を示すフローチャートである。

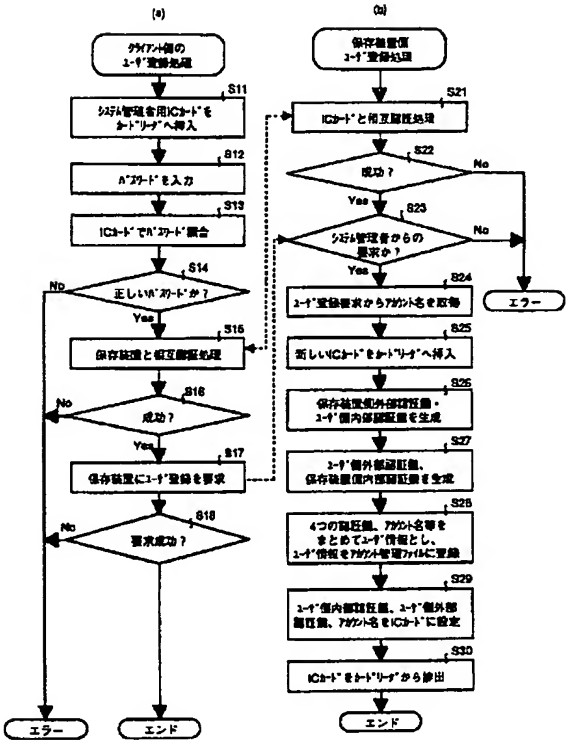
【符号の説明】

1　電子保存装置
2　計算機(クライアント)
3　ICカード
11　プロセッサ
12　通信ポート
13　大容量記憶媒体
14　プログラム格納媒体
15　内部記憶媒体
16　ICカードリーダ/ライタ
17　タイマ
21　データ
22　ファイル属性コード
23,27　ハッシュ値
24,28,33　メッセージ認証子
25　保存ファイル
26　ファイル属性情報
29　ファイル属性情報ファイル
31　保存ファイルリストファイル
32　保存ファイルリスト
34　リストハッシュ値
41　装置暗号鍵
42　装置復号鍵
43　タイマ設定履歴ファイル
44　アカウント管理ファイル

【図１】



【図２】



【図３】

アカウントエントリ#1	アカウント名
	アカウント登録日時情報
	アカウント抹消日時情報
	最終ログアウト日時情報
	保存装置側外部認証鍵情報
	ユーザ側内部認証鍵情報
	ユーザ側外部認証鍵情報
	保存装置側内部認証鍵情報
	登録抹消フラグ
	使用済みフラグ
アカウントエントリ#2	
アカウントエントリ#3	

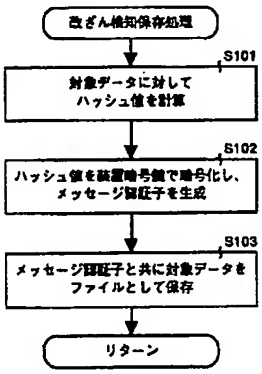
【図４】

鍵データ
鍵の長さ
アルゴリズム

【図５】

年
月
日
時
分
秒
タイマID

【図１０】



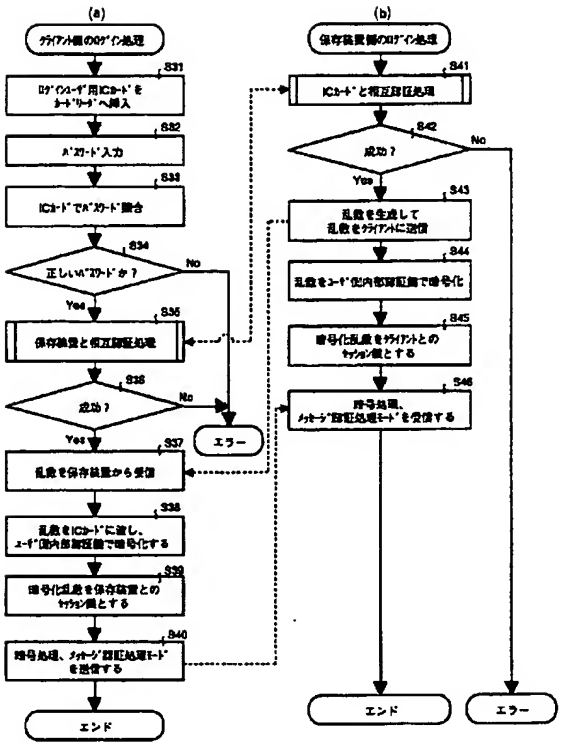
【図１２】

メッセージ認証子	
追記ブロック#1	追記データ長
	追記データ
追記ブロック#2	
追記ブロック#3	
...	

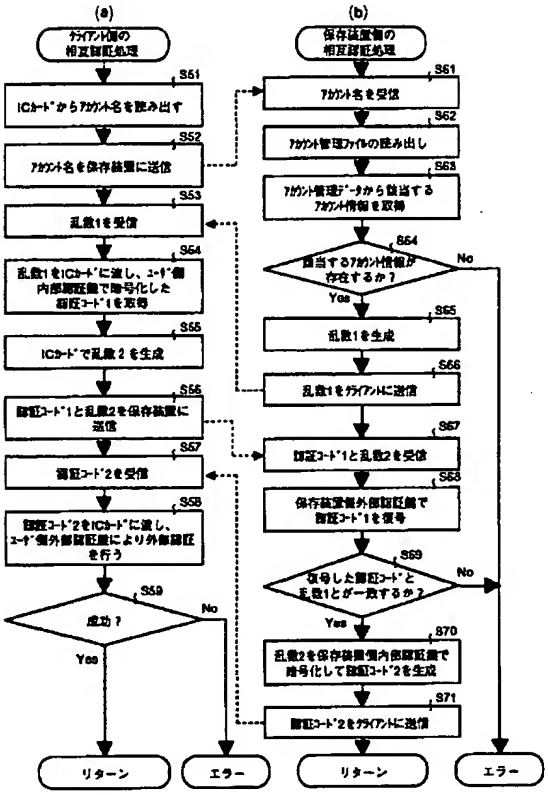
【図１５】

タイマ設定履歴#1	設定前の日時情報
	設定後の日時情報
	設定したユーザのアカウント名
タイマ設定履歴#2	
タイマ設定履歴#3	
...	

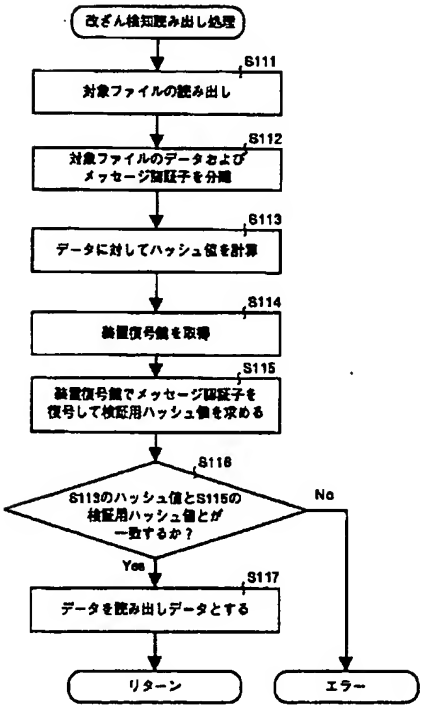
【図6】



【図7】



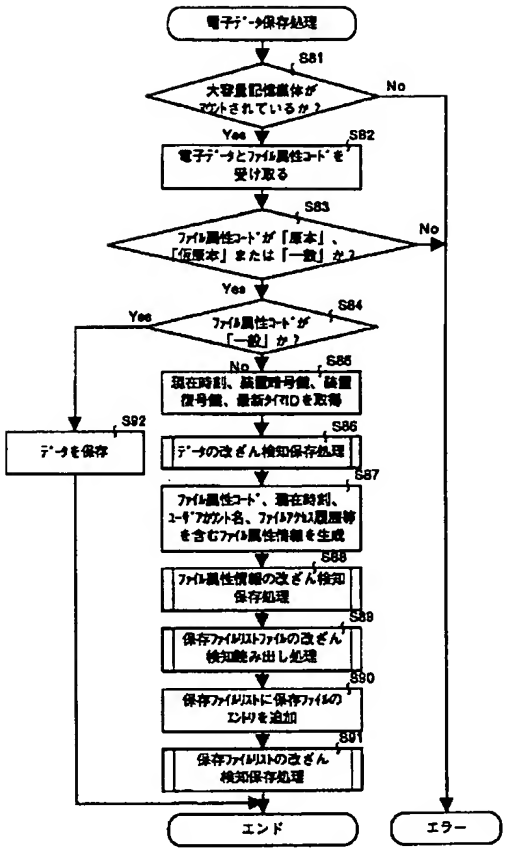
【図11】



【図13】

メッセージ認証子	
属性管理データ	ファイル名
	ファイルタイプ（ファイルまたはフォルダ）
	ファイルサイズ
	ファイルプロテクトモード（読み出し禁止、書込み禁止）
	ファイル属性コード（原本、謄本、仮原本）
	作成者アカウント名
	ファイル作成日時情報（タイマID含む）
	更新者アカウント名
	ファイル更新日時情報（タイマID含む）
アクセス履歴#1	アクセスユーザのアカウント名
	アクセス日時情報（タイマID含む）
	アクセス識別（作成、追記、原本化）
	保存装置識別番号
アクセス履歴#2	
アクセス履歴#3	
...	

【図８】



【図１４】

メッセージ識別子	
リストエントリ#1	有効・無効切り替えフラグ
	ファイル名
	フルパス名
	属性コード
	作成者アカウント名
	更新日時情報
	更新者アカウント名
	原本化実行者アカウント名
	原本化日時情報
	エントリ追加理由（原本化、原本作成、バックアップ作成、バックアップ復旧）
リストエントリ#2	
リストエントリ#3	
…	

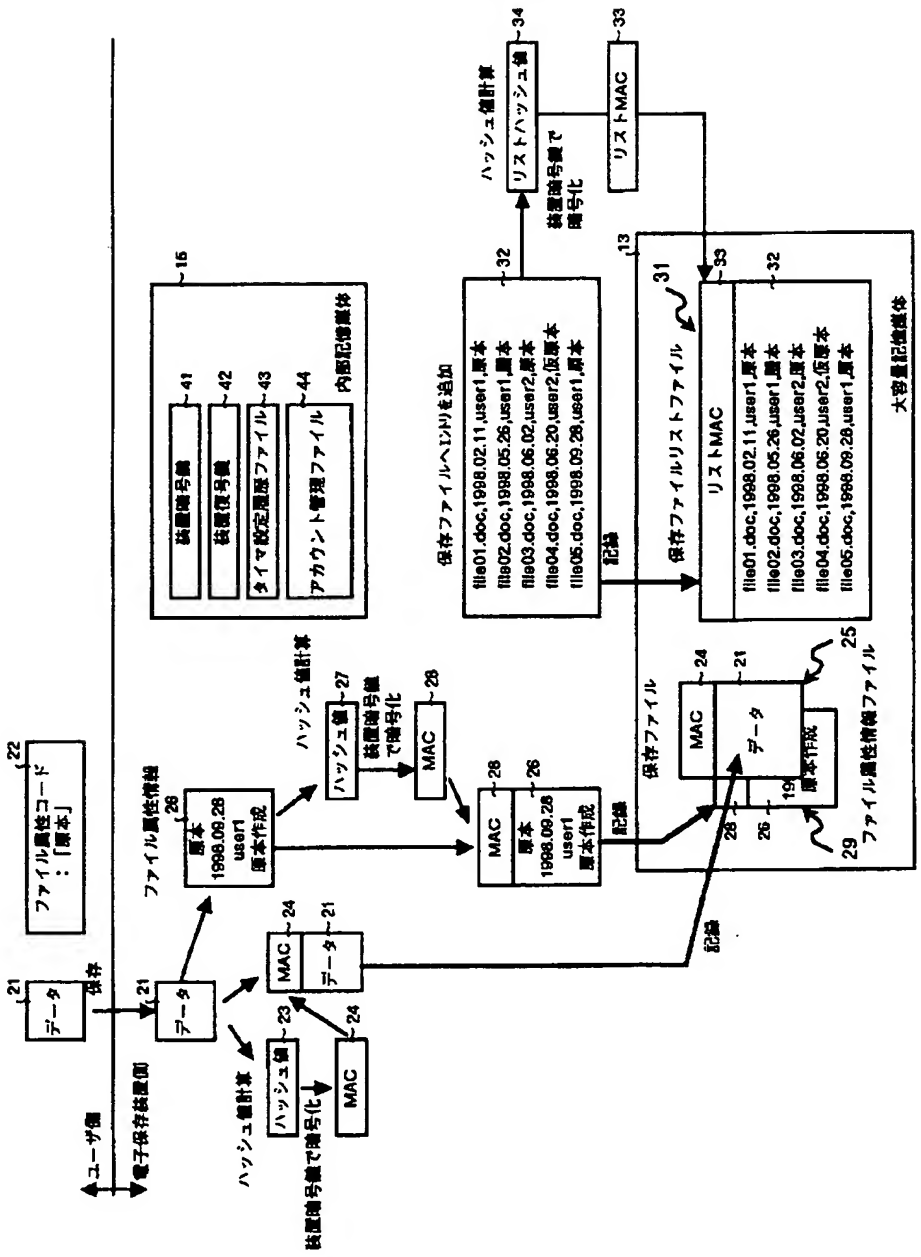
【図１６】

変更前	変更後
19990215 15:32:14 ID=1	19990215 15:30:00 ID=2
19990216 10:21:54 ID=2	19990116 10:22:00 ID=3
19990216 10:45:23 ID=3	19990216 10:46:00 ID=4

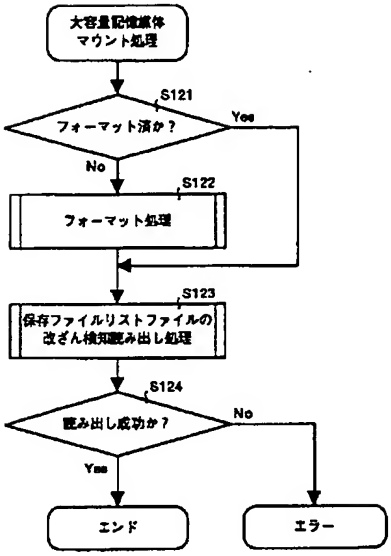
【図１７】

アクセス種別	アクセス日時	装置ID
CREATE	19990215 18:23:10 ID=1	R010-0001032
APPEND	19990215 18:23:30 ID=1	R010-0001032
MOVE TO	19990217 10:10:21 ID=3	R010-0001032
MOVE FROM	19990217 10:13:43 ID=2	R010-0001055

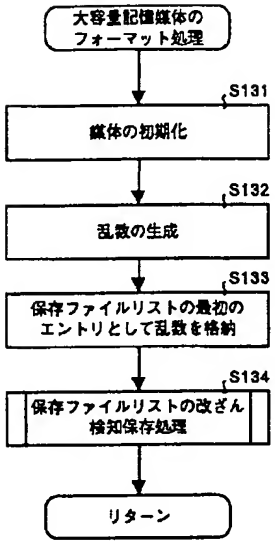
【図9】


ユーザ領
電子保存装置側
保存
データ
ファイル属性コード
：「原本」
ファイル属性情報
原本
1998.09.28
user1
原本作成
ハッシュ値計算
装置暗号鍵で暗号化
ハッシュ値
MAC
データ
装置暗号鍵
装置復号鍵
タイマ設定履歴ファイル
アカウント管理ファイル
内部記憶媒体
保存ファイルへエントリを追加
file01.doc,1998.02.11,user1,原本
file02.doc,1998.05.26,user1,原本
file03.doc,1998.06.02,user2,原本
file04.doc,1998.06.20,user2,仮原本
file05.doc,1998.09.28,user1,原本
記録
保存ファイルリストファイル
リストMAC
リストハッシュ値
大容量記憶媒体
ファイル属性情報ファイル
原本作成

【図18】



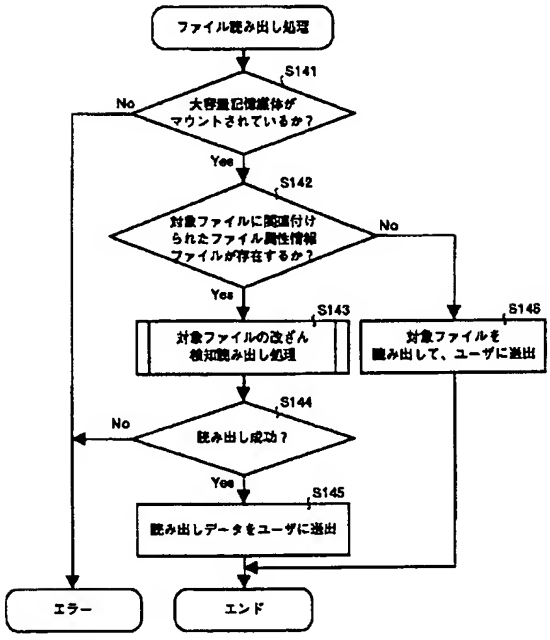
【図19】



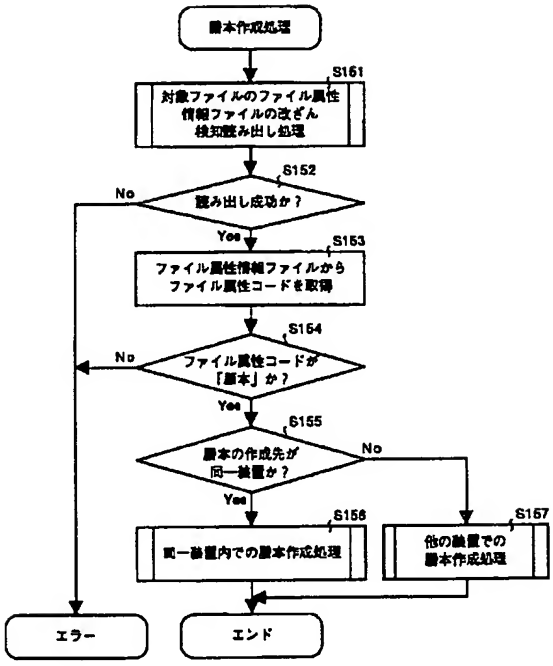
【図33】

復旧前	復旧後
謄本	原本
バックアップ仮原本	仮原本
バックアップ原本	原本
バックアップ謄本	謄本

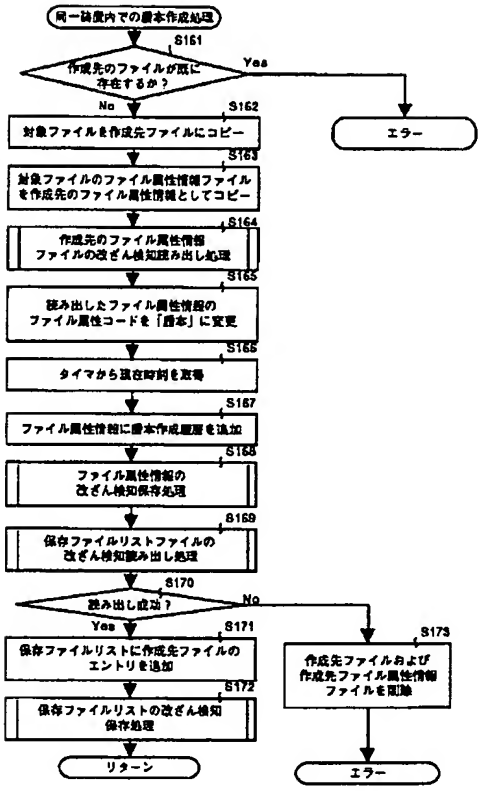
【図20】



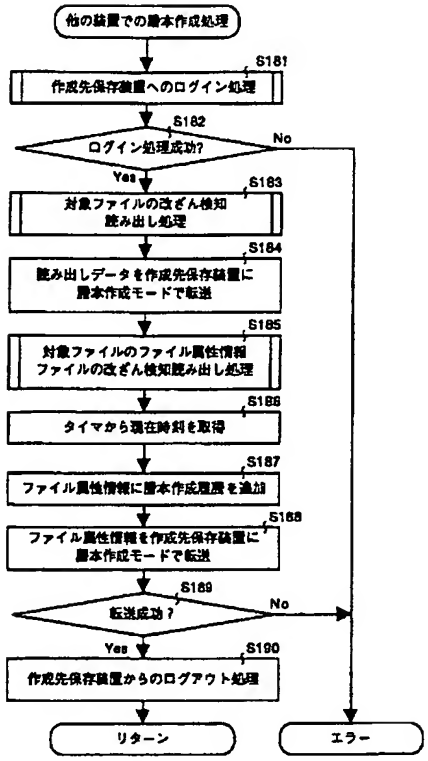
【図21】



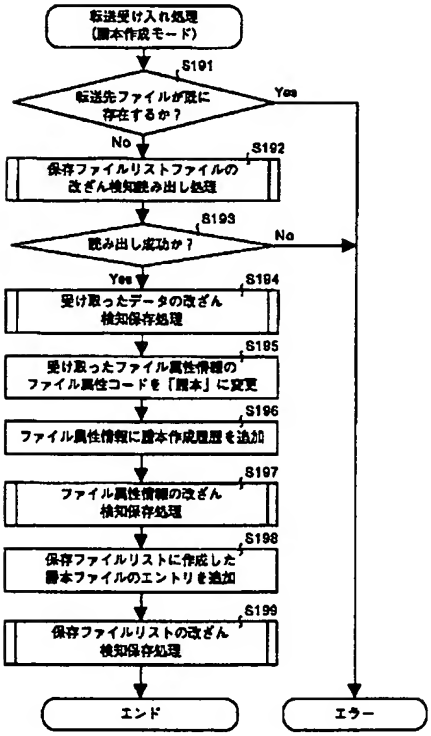
【図22】


同一装置内での原本作成処理
S161
作成先のファイルが既に存在するか？
Yes
No
S162
対象ファイルを作成先ファイルにコピー
S163
対象ファイルのファイル属性情報ファイルを作成先のファイル属性情報としてコピー
S164
作成先のファイル属性情報ファイルの改ざん検知読み出し処理
S165
読み出したファイル属性情報のファイル属性コードを「原本」に変更
S166
タイマから現在時刻を取得
S167
ファイル属性情報に原本作成履歴を追加
S168
ファイル属性情報の改ざん検知保存処理
S169
保存ファイルリストファイルの改ざん検知読み出し処理
S170
読み出し成功？
No
Yes
S171
保存ファイルリストに作成先ファイルのエントリを追加
S172
保存ファイルリストの改ざん検知保存処理
リターン
S173
作成先ファイルおよび作成先ファイル属性情報ファイルを削除
エラー
エラー

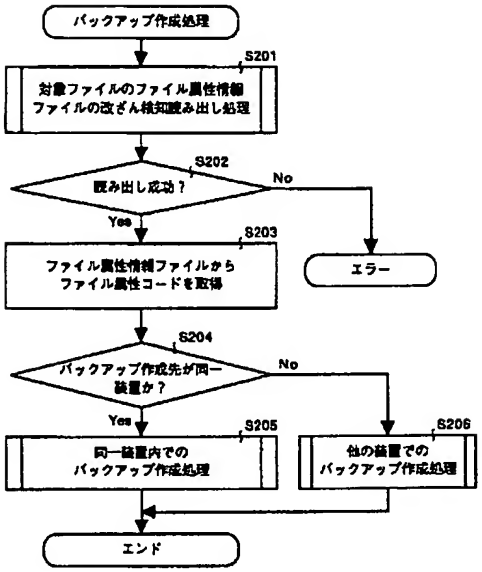
【図23】


他の装置での原本作成処理
S181
作成先保存装置へのログイン処理
S182
ログイン処理成功?
No
Yes
S183
対象ファイルの改ざん検知読み出し処理
S184
読み出しデータを作成先保存装置に原本作成モードで転送
S185
対象ファイルのファイル属性情報ファイルの改ざん検知読み出し処理
S186
タイマから現在時刻を取得
S187
ファイル属性情報に原本作成履歴を追加
S188
ファイル属性情報を作成先保存装置に原本作成モードで転送
S189
転送成功？
No
Yes
S190
作成先保存装置からのログアウト処理
リターン
エラー

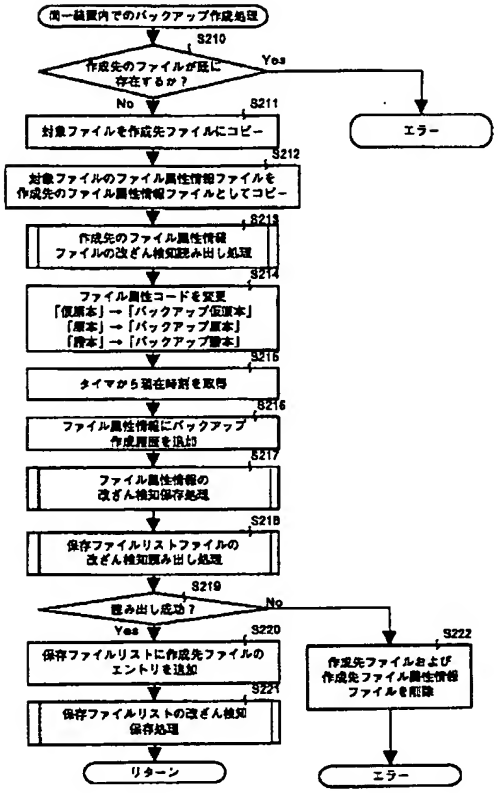
【図24】


転送受け入れ処理(原本作成モード)
S191
転送先ファイルが既に存在するか？
Yes
No
S192
保存ファイルリストファイルの改ざん検知読み出し処理
S193
読み出し成功か？
No
Yes
S194
受け取ったデータの改ざん検知保存処理
S195
受け取ったファイル属性情報のファイル属性コードを「原本」に変更
S196
ファイル属性情報に原本作成履歴を追加
S197
ファイル属性情報の改ざん検知保存処理
S198
保存ファイルリストに作成した原本ファイルのエントリを追加
S199
保存ファイルリストの改ざん検知保存処理
エンド
エラー

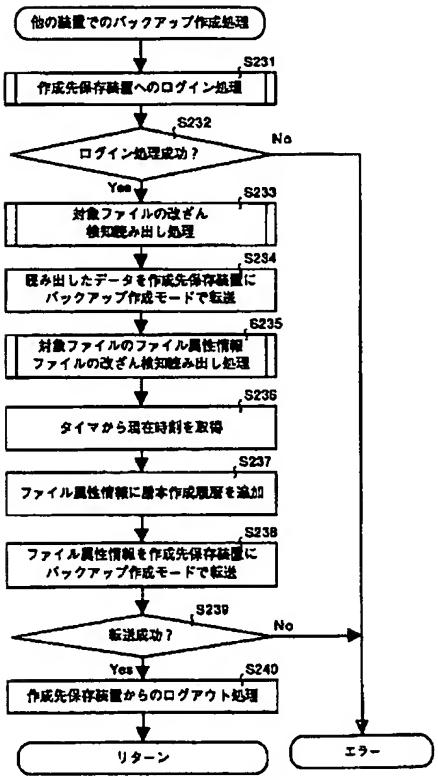
【図25】



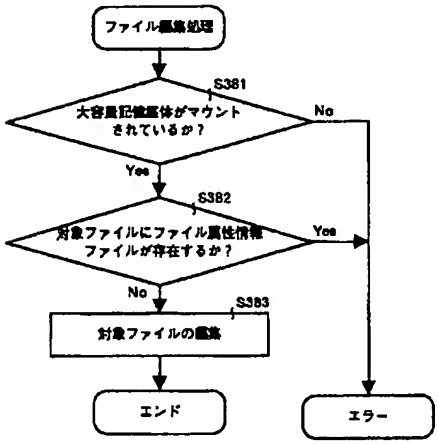
【図26】



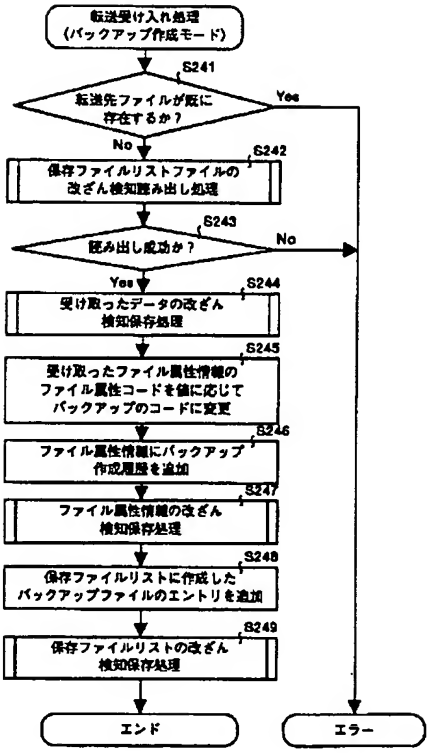
【図27】



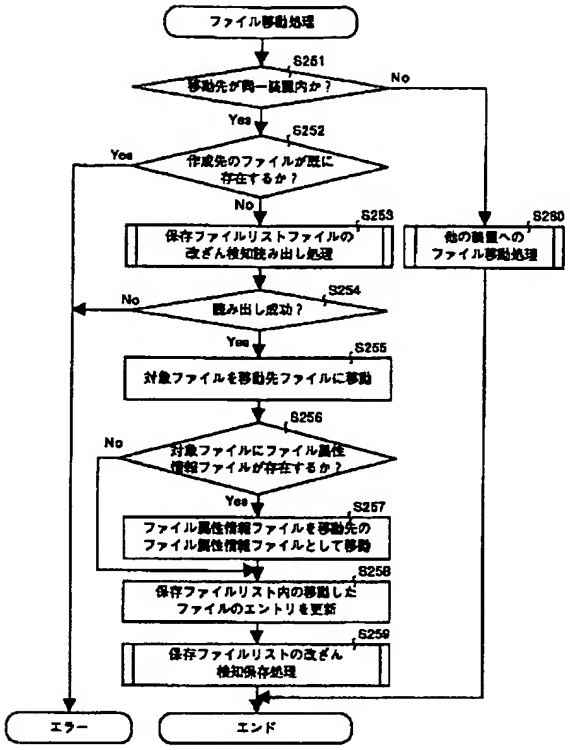
【図37】



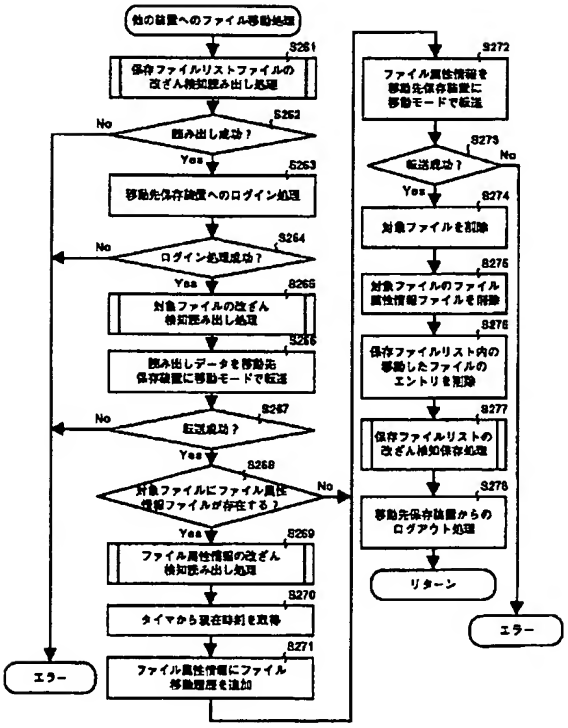
【図28】



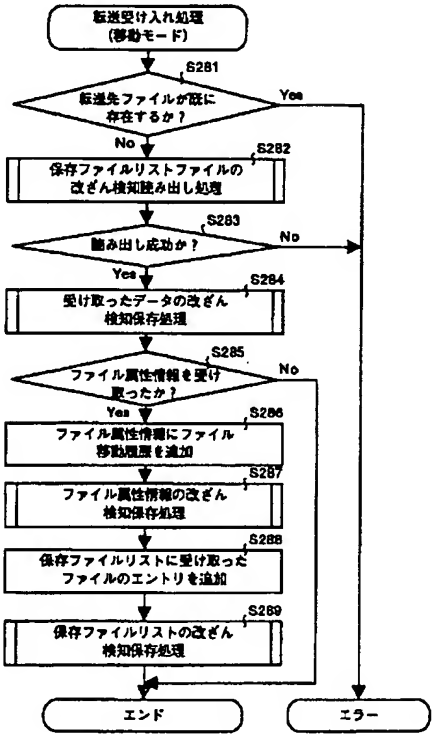
【図29】



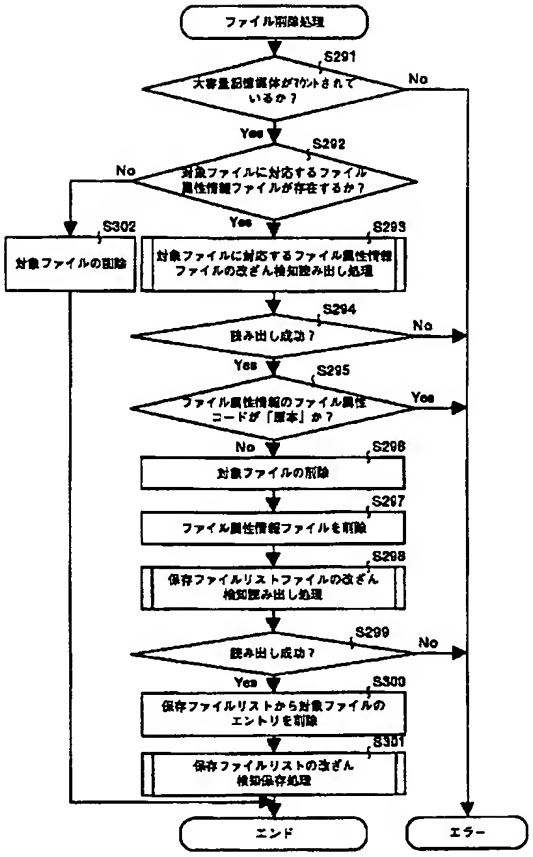
【図30】



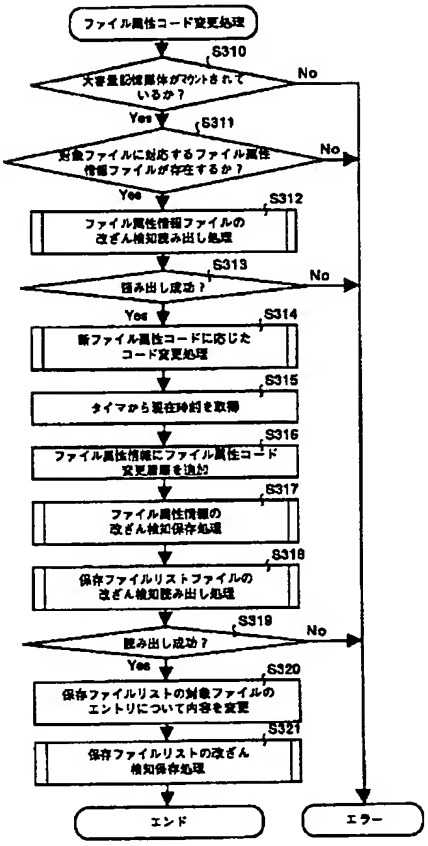
【図31】



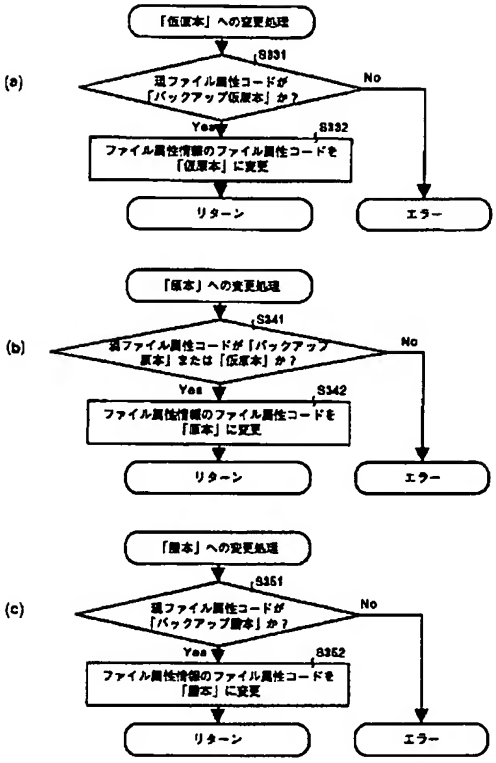
【図32】


ファイル削除処理
S291
大容量記憶媒体がマウントされているか？
No
Yes
S292
対象ファイルに対応するファイル属性情報ファイルが存在するか？
No
Yes
S302
対象ファイルの削除
S293
対象ファイルに対応するファイル属性情報ファイルのさざん検知読み出し処理
S294
読み出し成功？
No
Yes
S295
ファイル属性情報のファイル属性コードが「原本」か？
Yes
No
S296
対象ファイルの削除
S297
ファイル属性情報ファイルを削除
S298
保存ファイルリストファイルのさざん検知読み出し処理
S299
読み出し成功？
No
Yes
S300
保存ファイルリストから対象ファイルのエントリを削除
S301
保存ファイルリストのさざん検知保存処理
エンド
エラー

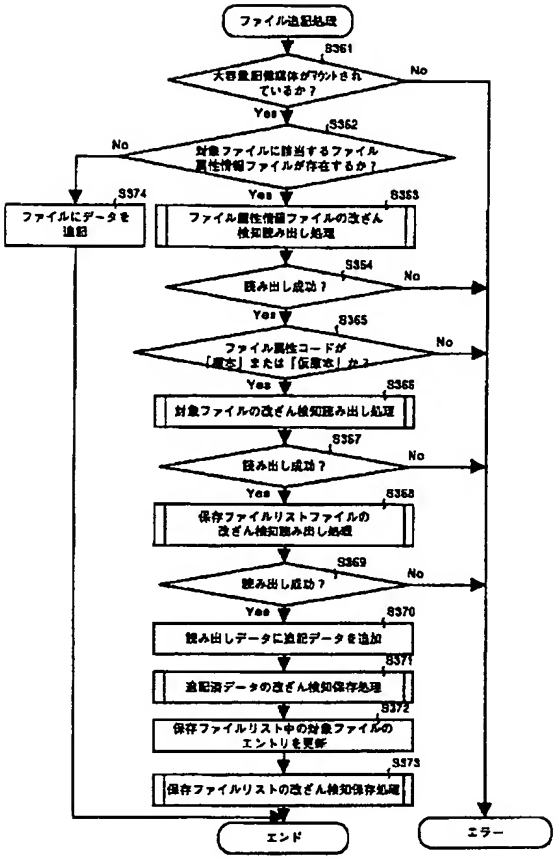
【図34】


ファイル属性コード変更処理
S310
大容量記憶媒体がマウントされているか？
No
Yes
S311
対象ファイルに対応するファイル属性情報ファイルが存在するか？
No
Yes
S312
ファイル属性情報ファイルのさざん検知読み出し処理
S313
読み出し成功？
No
Yes
S314
新ファイル属性コードに応じたコード変更処理
S315
タイマから現在時刻を取得
S316
ファイル属性情報にファイル属性コード変更履歴を追加
S317
ファイル属性情報のさざん検知保存処理
S318
保存ファイルリストファイルのさざん検知読み出し処理
S319
読み出し成功？
No
Yes
S320
保存ファイルリストの対象ファイルのエントリについて内容を変更
S321
保存ファイルリストのさざん検知保存処理
エンド
エラー

【図35】



【図36】



フロントページの続き

(72)発明者　谷内田　益義
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　菅生　清
東京都中央区勝関３丁目12番１号
(72)発明者　戸崎　英一
東京都中央区勝関３丁目12番１号

Ｆターム(参考)　5B017 AA01 BA05 BA06 BA07 BB10 CA16
5B082 AA11 EA10 EA12 GA02 GA13 GC05 HA08
5J104 AA08 LA02 NA12 NA35 PA00 PA14
9A001 BB04 CZ08 EZ03 HH33 LL03